

AD-A065 948

MICHIGAN UNIV ANN ARBOR DEPT OF INDUSTRIAL AND OPERA--ETC F/G 5/9  
URL/URA TRAINING EXAMPLE.(U)  
DEC 78

F19628-76-C-0197

NL

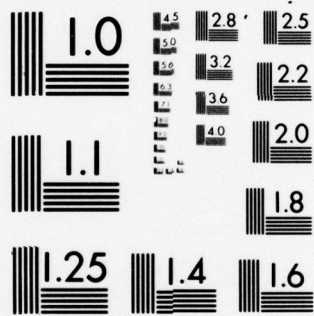
UNCLASSIFIED

ESD-TR-78-126

1 of 3

AD  
A095940



MICROCOPY RESOLUTION TEST CHART  
NATIONAL BUREAU OF STANDARDS-1963-A

ESD-TR-78-126

~~LEVEL~~

12



URL/URA TRAINING EXAMPLE

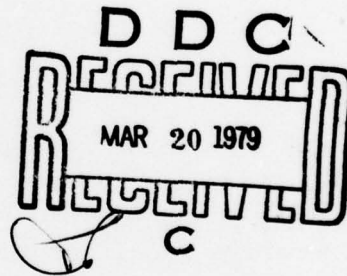
ISDOS Project  
University of Michigan  
Department of Industrial & Operations Engineering  
Ann Arbor, MI 48109

December 1978

AD A0 65948

DDC FILE COPY

Approved for Public Release;  
Distribution Unlimited.



THIS DOCUMENT IS BEST QUALITY PRACTICABLE.  
THE COPY FURNISHED TO DDC CONTAINED A  
SIGNIFICANT NUMBER OF PAGES WHICH DO NOT  
REPRODUCE LEGIBLY.

Prepared for

DEPUTY FOR TECHNICAL OPERATIONS  
ELECTRONIC SYSTEMS DIVISION  
HANSCOM AIR FORCE BASE, MA 01731

79 03 16 017

### LEGAL NOTICE

When U. S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

### OTHER NOTICES

Do not return this copy. Retain or destroy.

This Technical Report has been reviewed and is approved for publication.

*Charles J. Hartman*

CHARLES J. HARTMAN  
Technology Applications Division

*C. J. Grewe, Jr.*

CHARLES J. GREWE, Jr., Lt Colonel, USAF  
Chief, Technology Applications Division

FOR THE COMMANDER

*Normand Michaud*

NORMAND MICHAUD, Colonel, USAF  
Director, Computer Systems Engineering  
Deputy for Technical Operations

## **DISCLAIMER NOTICE**

**THIS DOCUMENT IS BEST QUALITY  
PRACTICABLE. THE COPY FURNISHED  
TO DDC CONTAINED A SIGNIFICANT  
NUMBER OF PAGES WHICH DO NOT  
REPRODUCE LEGIBLY.**

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM	
1. REPORT NUMBER ESD-TR-78-126	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER <i>Technical kept.</i>	
4. TITLE (and Subtitle) URL/URA TRAINING EXAMPLE,		5. TYPE OF REPORT & PERIOD COVERED Manual Jan 1976 to June 1976	
		6. REPORTING Q3G. REPORT NUMBER CDRL Item 007	
7. AUTHOR(s) ISDOS Project	8. CONTRACT OR GRANT NUMBER(s) F19628-76-C-0197		
9. PERFORMING ORGANIZATION NAME AND ADDRESS University of Michigan Department of Industrial & Operations Engineering Ann Arbor, Michigan 48109	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS PE 64740F, Project 2237		
11. CONTROLLING OFFICE NAME AND ADDRESS Deputy for Technical Operations Electronic Systems Division Hanscom AFB, MA 01731	12. REPORT DATE December 1978		
	13. NUMBER OF PAGES 252		
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) <i>12 250p.</i>	15. SECURITY CLASS. (of this report) UNCLASSIFIED		
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A		
16. DISTRIBUTION STATEMENT (of this Report) Approved for Public Release; Distribution Unlimited			
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)			
18. SUPPLEMENTARY NOTES			
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)			
Automated Tools		Requirements Analysis	
Computer-Aided Design		Requirements Language	
Information Processing		Requirements Specification	
Information System Requirements		Specification Analysis	
20. ABSTRACT (Continue on reverse side if necessary and identify by block number)			
<p>This manual is used during formal training of the Computer-Aided Design and Specification Analysis Tool (CADSAT). A requirements definition of a computer information system is constructed in steps. Examples of the database construction and analysis reports are shown. This report is a part of a series of CADSAT reports that explain the User Requirements Language (URL) and User Requirements Analyzer (URA).</p>			

# PREFACE

This manual is used during a formal five day training session. It describes the eight steps for developing a requirements definition of a computer information system. The database example is described in terms of URA version 3.0. Although the present version of the language is 3.3, the information described in this manual is upward compatible with 3.3. The example does not include some new reporting capability such as dynamic analysis, interval consistency, list changes, projected cost, resource consumption analysis, and security analysis. Refer to ESD Technical Report 78-130 and 78-131 for description of URL/URA Version 3.3.

A060517  
A058629  
A060780.

ACCESSION for	
NTIS	White Section <input checked="" type="checkbox"/>
PDC	Buff Section <input type="checkbox"/>
UNANNOUNCED	<input type="checkbox"/>
J S I LOCATION	
BY	
DISTRIBUTION/AVAILABILITY CODES	
SP. CIAL	
A	23

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION .....	1
I. IDENTIFICATION OF URL SYNTAX ERRORS BY URA .....	3
II. SYSTEM FLOW DESCRIPTION .....	4
III. SYSTEM PROPERTIES DESCRIPTION .....	6
IV. SYSTEM STRUCTURE DESCRIPTION.....	7
V. DATA STRUCTURE DESCRIPTION .....	10
VI. DATA DERIVATION DESCRIPTION .....	12
VII. SYSTEM SIZE DESCRIPTION .....	13
VIII. SYSTEM DYNAMICS DESCRIPTION.....	14
IX. PROJECT MANAGEMENT DESCRIPTION .....	15
X. ADDITIONAL REPORT EXAMPLES.....	16
XI. TECHNIQUES FOR MODIFYING A URA DATA BASE .....	18
XII. ADDITIONAL EXAMPLES OF NEW NAME GENERATION FACILITY..	19
APPENDIX.....	(see computer output page 21)

FIGURES

	<u>Page</u>
1. Correspondence between URL User's Manual Topics and Input Files in Example .....	2
2. System Diagram for Security Control System .....	5
3. Second-Level Diagram for Security Control System .....	8

## INTRODUCTION

The example described in this paper was selected for use as an aid in training Air Force personnel in the use of the User Requirements Language (URL) and User Requirements Analyzer (URA). It illustrates requirements definition for a security control system.

The purpose of the security control system is to allow users to access information for which they have a need and the necessary clearance, and to prevent unauthorized access. It must also allow security personnel to modify access privileges and to monitor system usage.

The example consists of a series of URL input files. Each contains information to be added to the data base containing all previous input. In this way, an incremental build-up of the system description in the URA data base is obtained.

Each input file illustrates a different aspect of the system description. This is useful for training purposes, but is not necessarily representative of the way in which a URA user would normally describe a system. In practice, the user should modify this scheme according to the needs of his own organization.

Each input file corresponds to a portion of Section 2 in the URL User's Manual, as shown in Figure 1. All the URL statements for a given aspect are contained in a single set of input. The As-Is Source Listing presents the contents of the input set, as input to URA. Following each As-Is Source Listing are several reports illustrating ways in which the information which exists in the data base at that point can be presented and analyzed.

In addition to the As-Is Source Listings and other reports mentioned above, the example contains As-Is Source Listings for input files containing syntax errors (pages 1-5) and reports produced as a result of URA commands which modify the data base (pages 207-217).

It should be noted that URA reports can be produced with various options. Not all of these are illustrated in the reports in this example. A description of all the options is given in the URL/URA User's Manual.

The remaining sections of this paper describe the various aspects of the example in more detail. The Appendix is the example itself, which consists of 223 pages of computer output.

9 03 16 047

Figure 1

Correspondence between URL User's Manual  
Topics and Input Files in Example

<u>Topic</u>	<u>Page numbers for As-Is Source Listing in example</u>
1. System flow	6
2. System properties	14-16
3. System structure	23-26
4. Data structure	41-54
5. Data derivation	75-86
6. System size	96-99
7. System dynamics	109-112
8. Project management	123-125

# I. IDENTIFICATION OF URL SYNTAX ERRORS BY URA (pages 1-5 of Appendix)

The example contains two As-Is Source Listings for URL input files containing syntax errors. These illustrate a number of errors that are detected by the Analyzer. A complete list of diagnostics is given in the URA User's Manual.

The URL statements in these files were input to URA using the UPDATE option, in order to show some of the errors which can be detected only by comparing input to information previously stored in the data base. This is not, in general, a good practice. Instead, the NOUPDATE option should be used for all input files which may contain syntax errors, in order to avoid the necessity of removing incorrect information from a URA data base. Once an input file has been checked by using the NOUPDATE option, the errors may be corrected and it may then be re-input using the UPDATE option to cause the data base to be modified.

## II. SYSTEM FLOW DESCRIPTION (pages 6-13 of Appendix)

The system flow description should define the system boundaries. All inputs to and outputs from the system should be named, along with those people, organizations, other systems, etc., which are outside the system boundaries but which generate inputs to the system or receive outputs from the system. Data bases used by the system should also be named. Connections between the objects named as part of the system flow description should be described.

The system flow description for the Security Control System, in the Appendix, corresponds to the picture of the system shown in Figure 2. The dotted lines in the figure indicate the system boundary.

The system flow portion of the Appendix consists of the following reports:

- As-is Source Listing with Cross Reference
- Name Generation
- Formatted Problem Statement
- Process Picture
- Interface Picture.

The As-Is Source Listing shows the URL system flow description, as input to URA. Since the UPDATE parameter was used, this information was used to update a URA data base, which was initially empty. The Cross Reference shows, for each name appearing in the As-Is Source Listing, the lines on which it appears.

Name Generation was used to produce a file containing all names in the URA data base. These names are listed, with their types, on the Name Generation report. This file of names was then used to produce a Formatted Problem Statement showing all information in the data base. This differs from the URL originally input, in that all complementary statements are shown.

Pictures are given to show graphically all relationships between security-control-system and security-control-interface and the other objects in the data base.

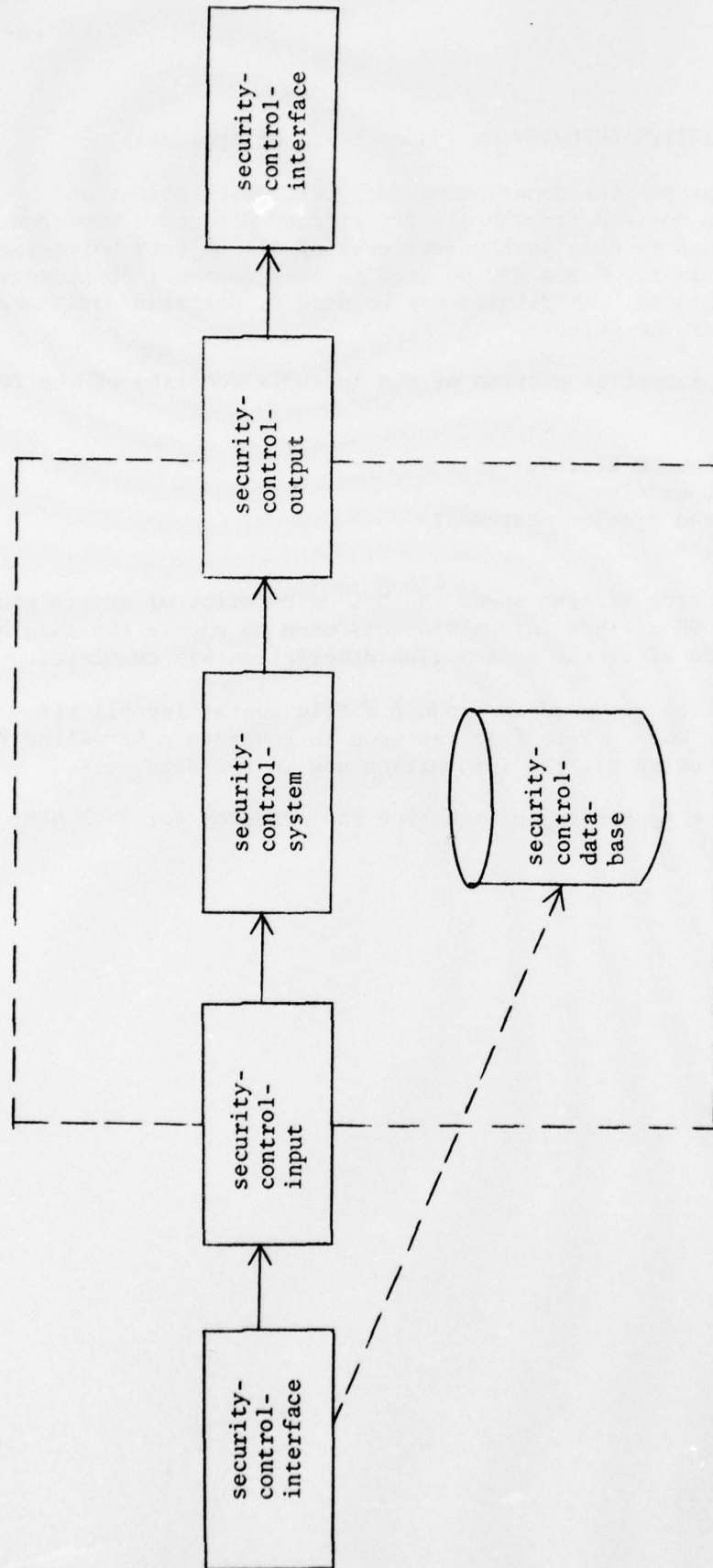


Figure 2  
System Diagram for Security Control System

### III. SYSTEM PROPERTIES DESCRIPTION (pages 14-22 of Appendix)

The system properties description adds text descriptions and any synonyms desired for the objects already defined. Keywords may be defined to help in the retrieval of all objects belonging to a given class. Memos may be used to make comments about certain groups of objects. Attributes may be used to describe additional properties of the objects.

The system properties portion of the Appendix consists of the following reports:

- As-Is Source Listing
- Name Generation
- Formatted Problem Statement
- Name List.

The As-Is Source Listing shows the URL description of system properties, as input to URA. This information was used to update the data base which existed after the system flow description was complete.

Name Generation was used to produce a file containing all names in the updated data base. This file was used to generate a Formatted Problem Statement showing all the information now in the data base.

The Name List report shows the type and synonyms for each name in the data base.

#### IV. SYSTEM STRUCTURE DESCRIPTION (pages 23-40 of Appendix)

The system structure description breaks the processing down into its major functions, and describes each of these with respect to system flow and system properties. Further information is given about data objects and their decomposition.

The system structure description for the example provides a good deal more detail about the security control system. This second-level description corresponds to the diagram in Figure 3. The names at the top and bottom of the diagram indicate the correspondence between Figure 2 (the top-level diagram) and Figure 3.

The following reports comprise the system structure portion of the Appendix:

- As-Is Source Listing
- Data Base Summary
- Process Structure
- Interface Structure
- Input Structure
- Output Structure
- Name Generation
- Formatted Problem Statement
- Name Generation
- Process Picture

The URL system structure description, as input to URA, is shown in the As-Is Source Listing. This information is added to the data base, which already contains the system flow and system properties descriptions.

The data base summary shows, for each type of name in the data base, the following:

- Number of names
- Number of names having synonyms
- Percentage of names having synonyms
- Number of names having descriptions
- Percentage of names having descriptions.

This is useful in evaluating the size and completeness of the data base.

Structure reports for the PROCESS security-control-system, the INTERFACE security-control-interface and the INPUT security-control-input show, in each case, how an object which is part of the top-level description of the problem is broken down into level-two objects.

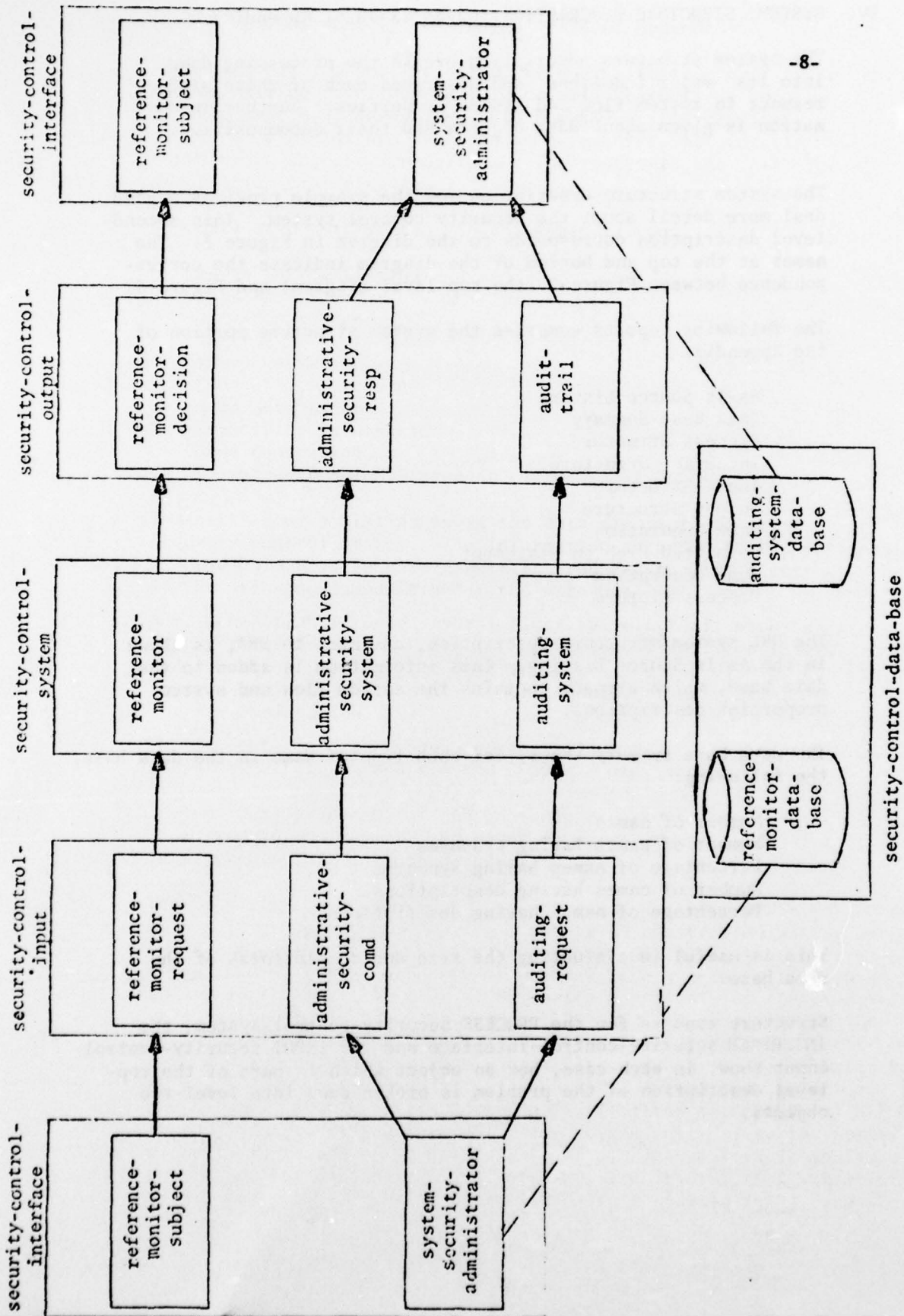


Figure 3

Second-Level Diagram for Security Control System

Name Generation is used to obtain all SET names from the data base, in order to obtain a Formatted Problem Statement for them.

Name Generation is used again to generate all PROCESSES, for use as input to the Picture report. The Picture reports for the PROCESSES now show both data flow information and structure information (PART, SUBPARTS).

## V. DATA STRUCTURE DESCRIPTION (pages 41-74 of Appendix)

Each data base, input, or output belonging to the security control system must be described in more detail. Each is decomposed, through as many levels as necessary, into ELEMENTS. All resulting names are given descriptions and synonyms as necessary. All relationships between the objects are defined. The result is the data structure description of the system.

The data structure section in the Appendix consists of the following:

- As-Is Source Listing
- Data Base Summary
- Name Generation
- Contents with Index
- Name Generation
- Consists Comparison
- Name Generation
- Identifier Information
- Name Generation
- Formatted Problem Statement

The As-Is Source Listing shows the data structure description for the security control system. The information is added to the data base, and the Data Base Summary report is produced to give a current picture of the size and composition of the data base.

Name Generation is used several times to select all names of a given type for the Contents, Consists Comparison, Identifier Information, and Formatted Problem Statement reports. The use of Name Generation to produce input for another report should, by this time, need no further explanation.

The Contents report is produced for all OUTPUTS, to show the breakdown for each OUTPUT, stated via the CONTAINS statement.

An Index was produced for the Contents report to show, for each name appearing in the report, the pages on which it was used. This feature is available for many other reports.

The Consists Comparison report was produced for all INPUTS in the data base. To produce the report, a matrix is constructed having one row for each INPUT. Each ELEMENT which is CONTAINED in one or more of these INPUTS, either directly or several levels down, will have a column in the matrix. (Any GROUPS which appear at the lowest level will be treated in the same way as ELEMENTS.) An asterisk in the (I, J) entry of the matrix indicates that the ELEMENT represented by column J is contained, directly or indirectly, in the INPUT represented by row I. In the second matrix, each INPUT corresponds to one row and one column. The entry in position (I, I) gives the number of ELEMENTS in the INPUT corresponding to I. The (I, J) entry gives the number of elements in common between INPUTS I and J. This matrix is analyzed to determine, for each pair (I, J) of INPUTS, whether I is a subset of J (i.e., each ELEMENT contained in I is also contained in J), and whether

I and J are equivalent (i.e., consist of the same ELEMENTS). This information can then be used by the analyst to determine whether the data base contains multiple names for a single INPUT, and whether some INPUTS should be SUBPARTS of others. The same report could be produced using SET, OUTPUT, ENTITY, and GROUP names, as well as INPUT names.

The Identifier Information report was produced for all the ENTITIES in the data base. That report consists of a matrix connecting ENTITIES and ELEMENTS which IDENTIFY them, followed by counts for the number of ENTITIES IDENTIFIED by each ELEMENT and the number of ELEMENTS which IDENTIFY each ENTITY.

A Formatted Problem Statement follows which shows all the information in the data base for each RELATION.

## VI. DATA DERIVATION DESCRIPTION (pages 75-95 of Appendix)

The data derivation description contains a much more detailed breakdown of the PROCESSES, and shows the ways in which various PROCESSES interact with data described in the data structure description to produce outputs.

This section of the Appendix shows the following:

- As-Is Source Listing
- Data Base Summary
- Name Generation
- Data Process Report
- Extended Picture

The URL input to describe data derivation is shown in the As-Is Source Listing. Once again, the data base is updated and the Data Base Summary report used to show the increase in available information.

The Data Process Report was produced with input consisting of all ELEMENTS in the data base. The result is a matrix showing the PROCESSES which USE or DERIVE each ELEMENT. The matrix is then used to find ELEMENTS which do not interact with any PROCESS and PROCESSES that have no inputs and/or outputs among the ELEMENTS. The Process Interaction Matrix is used to find PROCESSES with no predecessors and/or successors. The same report could be produced using any collection of SET, INPUT, OUTPUT, ENTITY, GROUP, and ELEMENT names.

The Extended Picture report was used to show data flow beginning at a specified PROCESS. Thus it shows all successors (direct or indirect) for that PROCESS, and all data objects used to determine predecessor-successor relationships.

## VII. SYSTEM SIZE DESCRIPTION (pages 96-108 of Appendix)

A number of components of a system require size and volume description. For example, the frequency with which a PROCESS is performed, the values of an ELEMENT, and the size of a SET must all be described in this way. These, and similar information, are included in the system size description.

The following reports are included in this section of the Appendix:

- As-Is Source Listing
- Data Base Summary
- Name Generation
- Formatted Problem Statement
- Name Generation
- Formatted Problem Statement
- Frequency Report

The As-Is Source Listing shows the URL input of system size information for our security control system example. The reader should note the use of SYSTEM-PARAMETERS to describe many quantifiable aspects of the system. A named SYSTEM-PARAMETER is essentially a variable representing some quantity which will be defined numerically later in the system design process, or which may vary.

Once again, the information shown in the As-Is Source Listing is added to the URA data base. The Data Base Summary reflects the continued growth of the data base.

Formatted Problem Statements are given for all SYSTEM-PARAMETERS and for all INTERVALS.

The Frequency Report shows, for a given INTERVAL, all objects which occur some number of times within that INTERVAL, along with the SYSTEM-PARAMETERS or integers which describe the frequency within the INTERVAL.

VIII. SYSTEM DYNAMICS DESCRIPTION (pages 109-122 of Appendix)

The system dynamics description deals with those aspects of the system which change over time. This includes EVENTS (which occur at instants of time), CONDITIONS (whose values may change over time), VOLATILITY (changeability) of ENTITIES and SETS, and the TRIGGERING of PROCESSES.

The following reports are included in the system dynamics section of the Appendix:

- As-Is Source Listing
- Data Base Summary
- Process Chain
- Name Generation
- Formatted Problem Statement
- Name Generation
- Formatted Problem Statement

The URL system dynamics description is shown in the As-Is Source Listing. This URL was input and stored in the data base, after which a Data Base Summary was run to indicate changes in the amount of information in the data base.

The Process Chain report shows the sequence of PROCESSES and EVENTS that occur as a result of the specified EVENT.

Formatted Problem Statements show all information in the data base related to all EVENTS and CONDITIONS in the data base.

IX. PROJECT MANAGEMENT DESCRIPTION (pages 13-135 of Appendix)

The project management description includes information on the people describing the system, and those portions of the system which each described, security information for the system description, sources of information, and any related memos.

This section of the Appendix contains the following:

- As-Is Source Listing
- Data Base Summary
- Name Generation
- Formatted Problem Statement
- Name Generation
- Dictionary Report
- Name Generation
- Punched Comment Entries.

The As-Is Source Listing shows project management information added to the data base. The Data Base Summary reflects the final state of the data base, now that the security control system has been described.

Name Generation is used to obtain all MAILBOX, MEMO, and PROBLEM-DEFINER names from the data base, in order to produce a Formatted Problem Statement. The reader should especially note the use of OR in the SELECTION parameter for Name Generation.

Name Generation is also used to obtain all URL objects described by the PROBLEM-DEFINER james-m-amster. The Dictionary Report then gives description, synonym, keyword, and responsible problem definer for each of these.

The descriptions for all MEMOS in the data base were punched. The Punched Comment Entries report shows the information that is contained in the resulting file. The process of punching comment entries is useful in correcting errors in comment entries, as will be demonstrated later in this paper.

X. ADDITIONAL REPORT EXAMPLES (pages 136-206 of Appendix)

The following additional report examples make use of the information in the complete Security Control System data base:

- Name List
- Name Generation
- Attribute Report
- Process Structure
- Name Generation
- Formatted Problem Statement
- Output Structure
- Name Generation
- Formatted Problem Statement
- Input Structure
- Name Generation
- Formatted Problem Statement
- Interface Structure
- Name Generation
- Formatted Problem Statement
- Name Generation
- Formatted Problem Statement
- Name Generation
- Formatted Problem Statement
- Kwic Index
- Consists Matrix Report
- Process Input/Output

The Name List report lists all names in the data base, along with their types and synonyms.

Name Generation was used to generate all ATTRIBUTE names from the data base. The Attribute Report then shows, for each of these, those names which it APPLIES TO and the corresponding ATTRIBUTE-VALUES.

The following reports were obtained for all PROCESSES, OUTPUTS, INPUTS, and INTERFACES:

- Structure
- Name Generation
- Formatted Problem Statement.

The reader should particularly note that all objects which are not part of larger objects appear at level one. This is useful in identifying names which have not yet been put into their proper places in the overall structure.

Formatted Problem Statements were also produced for all ENTITIES, ELEMENTS, and GROUPS in the system description.

The Kwic (Keyword in context) index is helpful in locating the names used to describe particular aspects of the target system and in identifying multiple names used to describe the same object.

The Consists Matrix shows, for each GROUP or ELEMENT, the GROUPS, ENTITIES, INPUTS, and OUTPUTS which CONTAIN it. This information is used to obtain counts of the number of objects which CONTAIN each GROUP or ELEMENT, and the number of GROUPS or ELEMENTS CONTAINED in each GROUP, ENTITY, INPUT, or OUTPUT. ENTITY, INPUT, and OUTPUT names may also be used as input to the Consists Matrix report.

The Process Input/Output report gives the DESCRIPTION and a full list of inputs and outputs for each PROCESS used as input to the command.

# XI. TECHNIQUES FOR MODIFYING A URA DATA BASE (pages 207-217 of Appendix)

The following reports demonstrate various techniques for making modifications to the data base:

- Change-Type Report
- Rename Report
- Deleted Comment Entries
- Deletion
- Replaced Comment Entries
- Deleted URL
- Formatted Problem Statement

Change-Type may be used to modify the type of a name that is already in the data base.

Rename may be used in a similar fashion to change a name. The new name must not, however, appear in the data base prior to the name change.

Delete-Comment-Entry may be used to remove specified comment-entries from the data base.

Replace-Comment-Entry replaces comment-entries currently in the data base with new ones. The reader should note that there is no way to edit comment-entries while they are a part of the data base; they may be altered only by replacement. Thus we can see the usefulness of Punch Comment Entry. It may be used to obtain a file of comment-entries for editing by the computer system editor. The edited comment-entries may then be re-input via Replace-Comment-Entry.

Delete-URL removes all relationships indicated in the URL used as input to the command. This is a "reversing" of the Input-URL process which adds information to the data base.

A Formatted Problem Statement is used to show the results of making the indicated changes to the security control system data base.

XII. ADDITIONAL EXAMPLES OF NEW NAME GENERATION FACILITY (pages 218-223 of Appendix)

Prior to July 1976, the Name Generation facility supplied with URA selected names such that each name satisfied one of the type parameters plus all of the additional selection parameters, such as SUB-PARTS-OF, KEY, and PD.

URA 3.0 allows more flexibility in specifying combinations of conditions for Name Generation. Legal values for the SELECTION parameter are discussed in the URA User's Manual. The examples in the Appendix illustrate some of the possibilities.

- A. SELECTION='KEY=level-2 AND PROCESS' generates all PROCESSES appearing at the second level.
- B. SELECTION=' (NOT PROCESS) \* KEY=level-2' generates all second level names except PROCESSES.
- C. SELECTION='ATTR=occurrences,unscheduled AND SO=security-control-input' chooses all subparts of security-control-input having unscheduled arrival times.
- D. SELECTION='(INPUT OR OUTPUT) \* ATTR=specder,implicit' selects all implicitly derived inputs and outputs.
- E. SELECTION='SO=security-control-input OR SO=security-control-output' generates all subparts of either the input or the output specified.

APPENDIX

for

URL/URA Training Example

ISDOS Working Paper No. 156

by

Claudia R. Stallings  
James M. Amster

ISDOS Research Project

Department of Industrial and Operations Engineering  
The University Of Michigan  
Ann Arbor, Michigan 48109  
313/763-3469, 763-5329

This document was prepared for the Air Force Electronic  
Systems Division under Contract F19628-76-C-0197.

REPRODUCTION PAGE NOT FILMED  
BLANK

## PREFACE

This Appendix consists of User Requirements Analyzer (URA) reports for a security control system example. The example was designed for use in a five day course on the User Requirements Language (URL) and User Requirements Analyzer.

Because this output was intended for training purposes, it may not be useful by itself. The body of Working Paper No. 156 contains a description and short explanations of the material in the Appendix. Students in the URL/URA course will receive more detailed instruction in its use.

## Table of Contents for URA Example

-23-

URA Report	Page
-----	----
AS-IS SOURCE LISTING (for System Flow errors)	1
AS-IS SOURCE LISTING (for System Properties errors)	3
AS-IS SOURCE LISTING (for System Flow)	6
CROSS REFERENCE (for above)	7
NAME GENERATION (for all names)	8
FORMATTED PROBLEM STATEMENT	9
PICTURE (for security-control-system)	10
PICTURE (for security-control-interface)	12
AS-IS SOURCE LISTING (for System Properties)	14
NAME GENERATION (for all names)	17
FORMATTED PROBLEM STATEMENT	18
NAME LIST	22
AS-IS SOURCE LISTING (for System Structure)	23
DATA BASE SUMMARY	27
STRUCTURE (for PROCESSES)	28
STRUCTURE (for INTERFACES)	29
STRUCTURE (for INPUTS)	30
STRUCTURE (for OUTPUTS)	31
NAME GENERATION (for SET names)	32
FORMATTED PROBLEM STATEMENT	33
NAME GENERATION (for PROCESS names)	35
PICTURES	36
AS-IS SOURCE LISTING (for Data Structure)	41
DATA BASE SUMMARY	55
NAME GENERATION (for OUTPUT names)	56
CONTENTS REPORT	57
INDEX (to CONTENTS REPORT)	60
NAME GENERATION (for INPUT names)	62
CONSISTS COMPARISON REPORT	63
NAME GENERATION (for ENTITY names)	69
IDENTIFIER INFORMATION REPORT	70
NAME GENERATION (for RELATION names)	72
FORMATTED PROBLEM STATEMENT	73
AS-IS SOURCE LISTING (for Data Derivation)	75
DATA BASE SUMMARY	87
NAME GENERATION (for ELEMENT names)	88
DATA PROCESS REPORT	89
EXTENDED PICTURE (for create-access-relation)	94
AS-IS SOURCE LISTING (for System Size)	96
DATA BASE SUMMARY	100
NAME GENERATION (for SYSTEM-PARAMETERS)	101
FORMATTED PROBLEM STATEMENT	102
NAME GENERATION (for INTERVAL names)	105
FORMATTED PROBLEM STATEMENT	106
FREQUENCY REPORT	108
AS-IS SOURCE LISTING (for System Dynamics)	109
DATA BASE SUMMARY	113
PROCESS CHAIN (for occur-release-usage-attr-req)	114
NAME GENERATION (for EVENT names)	117
FORMATTED PROBLEM STATEMENT	118
NAME GENERATION (for CONDITION names)	121
FORMATTED PROBLEM STATEMENT	122
AS-IS SOURCE LISTING (for Project Management)	123
DATA BASE SUMMARY	126
NAME GENERATION (for MEMO, MAILBOX and PROBLEM-DEFINER)	127

FORMATTED PROBLEM STATEMENT	128
NAME GENERATION (for PD=james-m-amster)	130
DICTIONARY REPORT	131
NAME GENERATION (for MFM names)	133
PUNCHED COMMENT ENTRIES	134
NAME LIST ORDER=BYTYPE	136
NAME GENERATION (for ATTRIBUTE names)	142
ATTRIBUTE REPORT	143
STRUCTURE (for PROCESSES)	144
NAME GENERATION (for PROCESSES)	146
FORMATTED PROBLEM STATEMENT	147
STRUCTURE (for OUTPUTS)	161
NAME GENERATION (for OUTPUTS)	162
FORMATTED PROBLEM STATEMENT	163
STRUCTURE (for INPUTS)	170
NAME GENERATION (for INPUTS)	171
FORMATTED PROBLEM STATEMENT	172
STRUCTURE (for INTERFACES)	179
NAME GENERATION (for INTERFACES)	180
FORMATTED PROBLEM STATEMENT	181
NAME GENERATION (for ENTITIES)	183
FORMATTED PROBLEM STATEMENT	184
NAME GENERATION (for GROUPS and ELEMENTS)	187
FORMATTED PROBLEM STATEMENT	188
KWIC INDEX	197
CONSISTS MATRIX REPORT	199
PROCESS INPUT/OUTPUT (for delete-object)	206
CHANGE TYPE REPORT	207
RENAME REPORT	208
DELETED COMMENT ENTRIES	209
DELETION	210
REPLACED COMMENT ENTRIES	211
DELETED URL	212
FORMATTED PROBLEM STATEMENT	213
NAME GENERATION (for level 2 PROCESS names)	218
NAME GENERATION (for level 2 non PROCESS names)	219
NAME GENERATION (for unscheduled subparts of security-control-input)	220
NAME GENERATION (for INPUT or OUTPUT names whose specification-derivation is implicit)	221
NAME GENERATION (for subparts of security-control-input or security-control-output)	222

## Security-control-example

## A S - T S S O U R C E L I S T I N G

PARAMETERS FOR: SYNJ

SOURCE NOXREF UPDATE DBRRP

LINE S T M T

ID FIELD

1 &gt; /\* SCS system flow \*/

2 &gt;

3 &gt; PROCESS: security-control-system;

4 &gt; RECEIVES: security-control-input; \$

\*\*\*\* RECEIVES

LEVEL 2,URA201:PLIST : NAME NOT PART OF HEADER \$

\*\*\*\* LEVEL 2,URA011:STACK : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - START SKIPPING \$

\*\*\*\* LEVEL 1,URA020:RECOV : LAST STATEMENT SKIPPED \$

5 &gt; GENERATES: security-control-output;

6 &gt;

7 &gt; INPUT: security-control-input;

8 &gt;

9 &gt; OUTPUT: security-control-output; \$

\*\*\*\* OUTPUT

LEVEL 2,URA201:PLIST : NAME NOT PART OF HEADER

LAST ERROR OCCURRED ON LINE 4 \$

\*\*\*\* LEVEL 2,URA011:STACK : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - START SKIPPING \$

\*\*\*\* LEVEL 1,URA020:RECOV : LAST STATEMENT SKIPPED \$

10 &gt;

11 &gt; INTERFACE: system-administrators-and-subjects; \$

\*\*\*\* LEVEL 1,URA002:NLEX : NAME TOO LONG

LAST ERROR OCCURRED ON LINE 9

12 &gt; GENERATES: security-control-input; \$

\*\*\*\* LEVEL 2,URA266:ILLST : ILLEGAL STATEMENT IN THIS SECTION

LAST ERROR OCCURRED ON LINE 11

13 &gt; RECEIVES: security-control-input; \$

\*\*\*\*

\*\*\*\*

\*\*\*\*

\*\*\*\*

\*\*\*\*

\*\*\*\*

\*\*\*\*

\*\*\*\*

URA VERSION 3.0P1

Security-control-example

JUN 16, 1976 00:49:28

PAGE

A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

\*\*\* Security-control-input

LEVEL 2, URA202:NLIST

: NAME PREVIOUSLY USED DIFFERENTLY - IGNORED

\*\*\*\*

LAST ERROR OCCURRED ON LINE 12

14 >

15 >

SFT:

Security-control-data-base;

16 >

\*\*\* LEVEL 1, URA003:NLFX

: EOF NOT FOUND BEFORE END-OF-FILE

\*\*\*\*

LAST ERROR OCCURRED ON LINE 13

## A S - I S S O U R C E L I S T I N G

## PARAMETERS FOR: SYMU

SOURCE NOXREF UPDATE DBREF

LINE S T M T

TD FIELD

```

1 > /* SCS system properties */
2 >
3 > PROCESS: security-control-system;
4 > SYNONYM: scs, scsvs;
5 > DESCRIPTION:
6 > The system will provide a means to allow users to process
7 > information concurrently while providing
8 > reasonable assurance that no unauthorized release of
9 > information shall take place. The security features must
10 > be an integral part of the operating system. The
11 > contractor can assume that the physical installation
12 > will be secured to the highest level of information in
13 > the system. ;
14 >
15 > INPUT: security-control-input;
16 > SYNONYM: scinp;
17 > DESCRIPTION
18 > The input to the security control system

**** LEVEL 2, URA011:STACK : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - STATE SKIPPING
19 > consists of requests by users to access and
20 > modify information in the system and of commands
21 > by security personnel to monitor the system. ;

**** LEVEL 1, URA020:PROCV : LAST STATEMENT SKIPPED
22 > LAST ERROR OCCURRED ON LINE 18
23 > OUTPUT: security-control-output;
24 > SYNONYM: scout;
25 > DESCRIPTION:
26 > The system will produce outputs of several
27 > different types: approvals to data access or modification
28 > requests, audit trails on security features, a
29 > record of outputs produced, etc. ;
30 >

```

## Security-control-example

A S - I S   S O U R C E   L I S T I N G

LINE S T M T

ID FIELD

31 > INTERFACE: security-control-interface:  
 32 > SYNONYM: scint,scout; \$

\*\*\*\* SCOUT

LEVEL 2,URA205:SETSUN : ALREADY SYNONYM FOR SOMETHING ELSE  
 LAST ERROR OCCURRED ON LINE 21  
 33 > PROCEDURE: \$

\*\*\*\*

\*\*\*\* LEVEL 2,URA266:ILLST : ILLEGAL STATEMENT IN THIS SECTION  
 LAST ERROR OCCURRED ON LINE 32

\*\*\*\*

34 > There will be several different types of users  
 35 > generating requests on the system and retrieving  
 36 > data from it. The security controls of the system  
 37 > must be capable of allowing users of different  
 38 > authorizations to process concurrently while preventing  
 39 > the release of information to unauthorized users. ;  
 40 >  
 41 > SET: security-control-data-base;  
 42 > SYNONYM: scdb,#1-file; \$

\*\*\*\* LEVEL 1,URA007:SCAN : ILLEGAL CHARACTER - IGNORED  
 LAST ERROR OCCURRED ON LINE 33

\*\*\*\*

\*\*\*\* LEVEL 1,URA007:SCAN : ILLEGAL CHARACTER - IGNORED

\*\*\*\*

\*\*\*\* LEVEL 2,URA011:STACK : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - START SKIPPING

\*\*\*\*

\*\*\*\* LEVEL 1,URA020:RECOV : LAST STATEMENT SKIPPED  
 DFDESCRIPTION:

\*\*\*\*

43 > The information in this set consists of all  
 44 > data stored and maintained by the security control  
 45 > system.  
 46 >  
 47 >

DFPINE: level-1 KEYWORD;  
 DESCRIPTION:

48 > This keyword is given to the highest level  
 49 > objects in the scs description. ;  
 50 >  
 51 > APPLIES: scs,scinp,scout,scint,scdb;  
 52 >

URA VERSION 3.091

Security-control-example

JUN 16, 1976 00:49:28

PAGE

5

A S - T S   S O U R C E   L I S T I N G

LINE S T M T

ID FIELD

\*\*\*\* LEVPL 2,URA266:ILLST : ILLEGAL STATEMENT IN THIS SECTION  
LAST ERROR OCCURRED ON LINE 42

53 >

54 > EOP

\*\*\*\*

## A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYN0

SOURCE XREF UPDATE DBREF

LINE S T M T

ID FIELD

```
1 > /* SCS system flow */
2 >
3 > PROCESS: security-control-system;
4 > RECEIVES: security-control-input;
5 > GENERATES: security-control-output;
6 >
7 > INPUT: security-control-input;
8 >
9 > OUTPUT: security-control-output;
10 >
11 > INTERFACE: security-control-interface;
12 > GENERATES: security-control-input;
13 > RECEIVES: security-control-output;
14 >
15 > SET: security-control-data-base;
16 > RESPONSIBLE-INTERFACE: security-control-interface;
17 >
18 > EOP
```

## Security-control-example.

## CROSS REFERENCE

## SEQ NAME

## TYPE

1 security-control-data-base	15	SET
2 security-control-input	4	INPUT 7 12
3 security-control-interface	11	INTERFACE 16
4 security-control-output	5	OUTPUT 9 13
5 security-control-system	3	PROCESS

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ALL' ORDER=BYTYPE

- |   |                            |           |
|---|----------------------------|-----------|
| 1 | security-control-input     | INPUT     |
| 2 | security-control-interface | INTERFACE |
| 3 | security-control-output    | OUTPUT    |
| 4 | security-control-system    | PROCESS   |
| 5 | security-control-data-base | SET       |

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNARG=70 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONEX-PAGE NONEX-LINE

```

1 INPUT
2   GENERATED BY:
3   RECEIVED BY:
4
5 INTERFACE
6   GENERATES:
7   RECEIVES:
8   RESPONSIBLE FOR:
9
10 OUTPUT
11  GENERATED BY:
12  RECEIVED BY:
13
14 PROCESS
15  RECEIVES:
16  GENERATES:
17
18 SPT  RESPONSIBLE-INTERFACE IS:
19
20
21 EOF EOF EOF EOF

```

security-control-input;  
 security-control-interface;  
 security-control-system;  
  
 security-control-interface;  
 security-control-input;  
 security-control-output;  
 security-control-data-base;  
  
 security-control-output;  
 security-control-system;  
 security-control-interface;  
  
 security-control-system;  
 security-control-input;  
 security-control-output;  
  
 security-control-data-base;  
 security-control-interface;

TRA VERSION 3.0P1

PAGE 10

JUN 16, 1976 00:49:28

Security-control-example

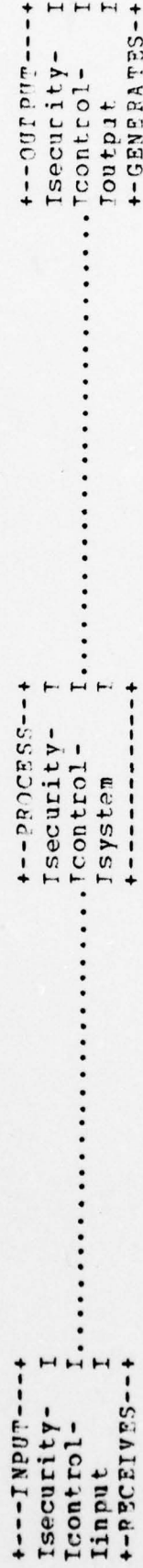
PICTURE

PARAMETERS FOR: PIC

NAME=security-control-system NOINDEX DATA STRUCTURE FLOW

PROCESS PICTURE

security-control-system



URA VERSION 3.0R1

Security-control-example

JUN 16, 1976 00:49:28

PAGE

12

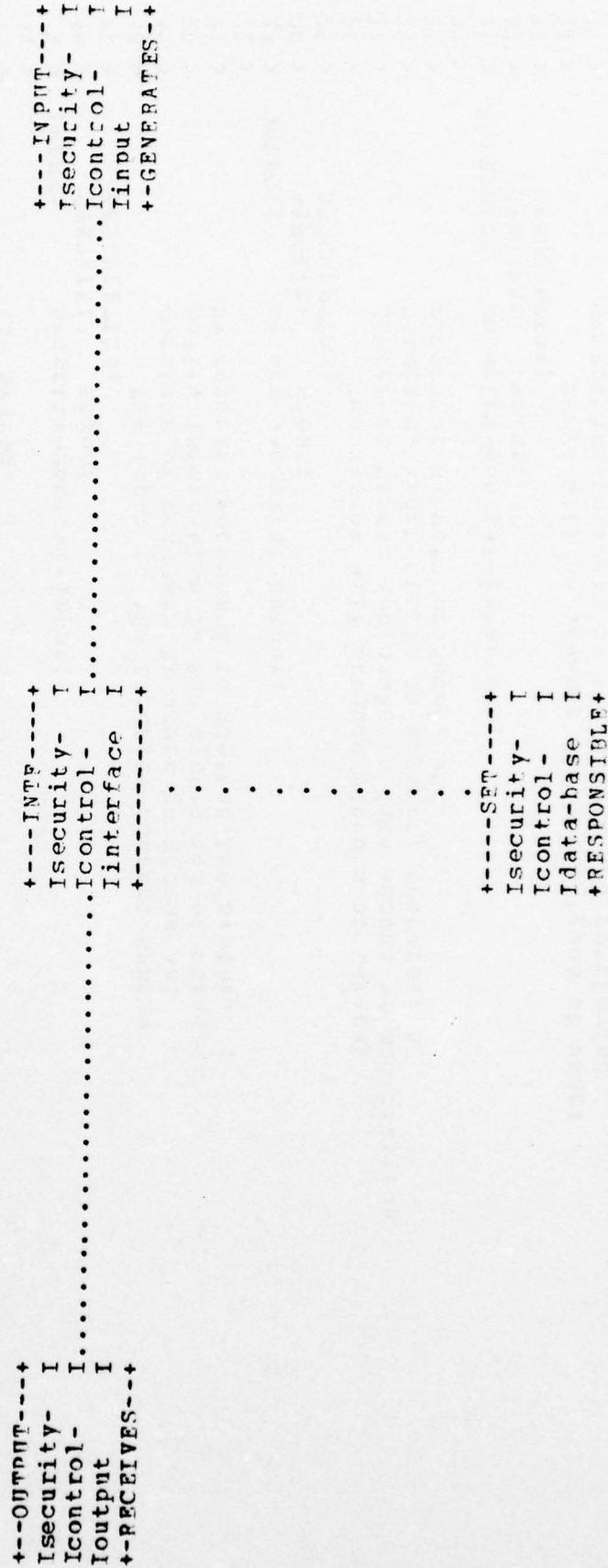
PICTURE

PARAMETERS FOR: PIC

NAME=security-control-interface NOINDEX DATA STRUCTURE FLOW

INTERFACE PICTURE

security-control-interface



## A S - I S S O U R C E L I S T I N G

## PARAMETERS FOR: SYNT

## SOURCE NOXREF UPDATE DBREF

## LINE S T M T

## ID FIELD

```

1 > /* SCS system properties */
2 >
3 > PROCESS: security-control-system;
4 > SYNONYM: SCS, SCSYS;
5 > DESCRIPTION: The system will provide a means to allow users to
6 > process information concurrently while providing
7 > reasonable assurance that no unauthorized release of
8 > information shall take place. The security features must
9 > be an integral part of the operating system. The
10 > contractor can assume that the physical installation
11 > will be secured to the highest level of information in
12 > the system. ;
13 >
14 >
15 > INPUT: security-control-input;
16 > SYNONYM: scinp;
17 > DESCRIPTION: The input to the security control system
18 > consists of requests by users to access and
19 > modify information in the system and of commands
20 > by security personnel to monitor the system. ;
21 >
22 >
23 > OUTPUT: security-control-output;
24 > SYNONYM: scout;
25 > DESCRIPTION: The system will produce outputs of several
26 > different types: approvals to data access or modification
27 > requests, audit trails on security features, a
28 > record of outputs produced, etc. ;
29 >
30 >
31 > INTERFACE: security-control-interface;
32 > SYNONYM: scint;
33 > DESCRIPTION: There will be several different types of users
34 > generating requests on the system and retrieving
35 >

```

## A S - T S S O U R C E L I S T I N G

TO FIELD

LINE S T M T

```

36 > data from it. The security controls of the system
37 > must be capable of allowing users of different
38 > authorizations to process concurrently while preventing
39 > the release of information to unauthorized users. ;
40 >
41 > SET: security-control-data-base;
42 > SYNONYM: scdb;
43 > DESCRIPTION;
44 > The information in this set consists of all
45 > data stored and maintained by the security control
46 > system. ;
47 >
48 >
49 > DEFINE: level-1 KEYWORD;
50 > DESCRIPTION;
51 > This keyword is given to the highest level
52 > objects in the scs description. ;
53 > APPLIPS: scs,scinp,scout,scint,scdb;
54 >
55 > MEMO: system-philosophy-memo;
56 > DESCRIPTION;
57 > The philosophy of the secure computer system will
58 > be such that the system will control the various shared
59 > resources. Hence the user will only be able to influence
60 > allocation decisions in a secondary way. Specifically,
61 > he can ask for a resource but not control the absolute
62 > time or address of the resource. It is essential that any
63 > other paths which might allow the user to access
64 > information (from any device) without the access controls
65 > of the system be eliminated. ;
66 > APPLIPS: scs,scinp,scout,scint,scdb;
67 >
68 > DEFINE: specification-derivation ATTRIBUTE;
69 > SYNONYM: specifier;
70 > DESCRIPTION;
71 > This attribute specifies whether a complete and
72 > explicit description of the object can be found in
73 > current documentation of the system or whether it
74 > must be derived from this documentation. ;

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```
75 >
76 > PROCESS: scs;
77 > ATTRIBUTE: specder explicit;
78 >
79 > INPUT: scinp;
80 > ATTRIBUTE: specder implicit;
81 >
82 > OUTPUT: scout;
83 > ATTRIBUTE: specder implicit;
84 >
85 > INTERPACE: scint;
86 > ATTRIBUTE: specder explicit;
87 >
88 > SET: scdb;
89 > ATTRIBUTE: specder implicit;
90 >
91 > EOP
```

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ALL' ORDER=BYTYPE

1	specification-derivation	ATTRIBUTE
2	explicit	ATTRIBUTE-VALUE
3	implicit	ATTRIBUTE-VALUE
4	security-control-input	INPUT
5	security-control-interface	INTERFACE
6	level-1	KEYWORD
7	system-philosophy-memo	MEMO
8	security-control-output	OUTPUT
9	security-control-system	PROCESS
10	security-control-data-base	SET

PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=70 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONEX-PAGE NONEX-LINE

```

1 DEFINE
2   AS A ATTRIBUTE;
3 /* VALUES ARE:
4   explicit FOR
5   implicit FOR
6   implicit FOR
7   explicit FOR
8   implicit FOR
9 */
10  SYNONYMS ARE:
11  DESCRIPTION;
12
13  This attribute specifies whether a complete and
14  explicit description of the object can be found in
15  current documentation of the system or whether it
16  must be derived from this documentation.;
17
18  DEFINE
19    AS A ATTRIBUTE-VALUE;
20
21  DEFINE
22    AS A ATTRIBUTE-VALUE;
23
24  INPUT
25    SYNONYMS ARE:
26    DESCRIPTION;
27
28    The input to the security control system
29    consists of requests by users to access and
30    modify information in the system and of commands
31    by security personnel to monitor the system.;
32
33  SEE-MEMO:
34  KEYWORDS:
35  ATTRIBUTES ARE:
36    specification-derivation
37    GENERATED BY:
38    RECEIVED BY:
39
40  implicit;
41  security-control-interface;
42  security-control-system;
43
44  security-control-system,
45  security-control-input,
46  security-control-output,
47  security-control-interface,
48  security-control-data-base,
49
50  specification-derivation
51
52  specifier;
53
54  security-control-input;
55  scinp;
56
57  security-control-input;
58  scinp;
59
60  security-control-input;
61  scinp;
62
63  security-control-input;
64  scinp;
65
66  security-control-input;
67  scinp;
68
69  security-control-input;
70  scinp;
71
72  security-control-input;
73  scinp;
74
75  security-control-input;
76  scinp;
77
78  security-control-input;
79  scinp;
80
81  security-control-input;
82  scinp;
83
84  security-control-input;
85  scinp;
86
87  security-control-input;
88  scinp;
89
90  security-control-input;
91  scinp;
92
93  security-control-input;
94  scinp;
95
96  security-control-input;
97  scinp;
98
99  security-control-input;
100 scinp;

```

## FORMATTED PROBLEM STATEMENT

37 INTERPACE  
 38 SYNONYMS ARE:  
 39 DESCRIPTION:  
 40  
 41 There will be several different types of users  
 42 generating requests on the system and retrieving  
 43 data from it. The security controls of the system  
 44 must be capable of allowing users of different  
 45 authorizations to process concurrently while preventing  
 46 the release of information to unauthorized users.;  
 47  
 48 SFE-MEMO:  
 49 security-control-interface;  
 50 scint;  
 51  
 52 KEYWORDS:  
 53  
 54 ATTRIBUTES ARE:  
 55 specification-derivation  
 56  
 57 GENERATES:  
 58 explicit;  
 59 security-control-input;  
 60 security-control-output;  
 61 security-control-data-base;  
 62  
 63 RECEIVES:  
 64  
 65 RESPONSIBLE FOR:  
 66  
 67  
 68  
 69  
 70  
 71  
 72  
 73  
 74  
 75  
 76  
 77

54 DEFINE  
 55 AS A KEYWORD;  
 56 DESCRIPTION:  
 57  
 58 This keyword is given to the highest level  
 59 objects in the scs description.;  
 60  
 61 security-control-system,  
 62 security-control-input,  
 63 security-control-output,  
 64 security-control-interface,  
 65 security-control-data-base;  
 66  
 67  
 68  
 69  
 70  
 71  
 72  
 73  
 74  
 75  
 76  
 77

65 MEMO  
 66 DESCRIPTION:  
 67  
 68 The philosophy of the secure computer system will  
 69 be such that the system will control the various shared  
 70 resources. Hence the user will only be able to influence  
 71 allocation decisions in a secondary way. Specifically,  
 72 he can ask for a resource but not control the absolute  
 73 time or address of the resource. It is essential that any  
 74 other paths which might allow the user to access  
 75 information (from any device) without the access controls  
 76 of the system be eliminated.;  
 77  
 78  
 79  
 80  
 81  
 82  
 83  
 84  
 85  
 86  
 87  
 88  
 89  
 90  
 91  
 92  
 93  
 94  
 95  
 96  
 97  
 98  
 99  
 100

APPLIES TO:  
 security-control-system,  
 security-control-input,

## FORMATTED PROBLEM STATEMENT

78 security-control-output,  
 79 security-control-interface,  
 80 security-control-data-base;  
 81  
 82 security-control-output;  
 83 scout;  
 84  
 85 The system will produce outputs of several  
 86 different types: approvals to data access or modification  
 87 requests, audit trails on security features, a  
 88 record of outputs produced, etc.;

89 system-philosophy-memo;  
 90 level-1;  
 91 implicit;  
 92 security-control-system;  
 93 security-control-interface;  
 94  
 95 security-control-system;  
 96 SCS,  
 97 SCSYS;  
 98  
 99 The system will provide a means to allow users to  
 100 process information concurrently while providing  
 101 reasonable assurance that no unauthorized release of  
 102 information shall take place. The security features must  
 103 be an integral part of the operating system. The  
 104 contractor can assume that the physical installation  
 105 will be secured to the highest level of information in  
 106 the system.;

107 system-philosophy-memo;  
 108 level-1;  
 109 explicit;  
 110 security-control-input;  
 111 security-control-output;  
 112  
 113 security-control-data-base;  
 114 scdb;  
 115  
 116 The information in this set consists of all  
 117  
 118

Security-control-example

FORMATTED PROBLEM STATEMENT

```

119      data stored and maintained by the security control
120      system.;
121      SPE-MEMO:
122      KEYWORDS:
123      ATTRIBUTES ARE:
124      specification-derivation
125      RESPONSIBLE-INTERFACE IS:
126
127 EOF EOF EOF EOF EOF

```

system-philosophy-memo;  
level-1;

implicit;  
security-control-interface;

NAME LIST

PARAMETERS FOR: NL

ORDER=ALPHA

NAME	TYPE	SYNONYM
1 explicit	ATTRIBUTE-VALUE	
2 implicit	ATTRIBUTE-VALUE	
3 level-1	KEYWORD	
4 security-control-data-base	SPT	sldb
5 security-control-input	INPUT	scinp
6 security-control-interface	INTERFACE	scint
7 security-control-output	OUTPUT	scout
8 security-control-system	PROCESS	scs
9 specification-derivation	ATTRIBUTE	scsys
10 system-philosophy-memo	MEMO	specder

## A S - I S S O U R C E L I S T I N G

## PARAMETERS FOR: SYNU

## SOURCE NOXREF UPDATE DBREF

## LINE S T M T

## ID FIELD

```

1 > /* SCS system structure */
2 >
3 > PROCESS: SCS;
4 > SUBPARTS: reference-monitor,
5 > administrative-security-system,
6 > auditing-system;
7 >
8 > PROCESS: reference-monitor;
9 > SYNONYM: access-control-system, rmon;
10 > DESCRIPTION;
11 > The system will provide controls which will allow
12 > users to operate concurrently while preventing the
13 > release of information to unauthorized users. The
14 > system will also prevent inadvertent violation of need
15 > to know access to data. In addition to providing the
16 > primary access controls for this environment, the
17 > system will provide programs which perform subsidiary
18 > security control functions.
19 > The capability must be provided for the system
20 > hardware to check the validity of all arguments
21 > utilized in calling the operating system. ;
22 > RECEIVES: reference-monitor-request;
23 > GENERATES: reference-monitor-decision;
24 >
25 > PROCESS: administrative-security-system;
26 > SYNONYM: admssys;
27 > DESCRIPTION;
28 > The system will define the administrative
29 > functions of the system security administrator, and will
30 > support his responsibility for maintaining control of
31 > users id's, passwords, and user classification level and
32 > category set. ;
33 > RECEIVES: administrative-security-command;
34 > GENERATES: administrative-security-response;
35 >

```

## A S - I S S O U R C E L I S T I N G

## LINE S T M T

## ID FIELD

```

36 > PROCESS: auditing-system;
37 > SYNONYM: aidsys;
38 > DESCRIPTION:
39 > The system will provide an automatic capability to
40 > collect and record data regarding security related
41 > actions. ;
42 > RECEIVES: auditing-request;
43 > GENERATES: audit-trail;
44 >
45 > INPUT: reference-monitor-request;
46 > SYNONYM: rmonreq;
47 > DESCRIPTION:
48 > These are requests to access or modify information
49 > in the system and may include output options. ;
50 > ATTRIBUTE: occurrences unscheduled;
51 > PART OF: security-control-input;
52 >
53 > OUTPUT: reference-monitor-decision;
54 > SYNONYM: rmondec;
55 > DESCRIPTION:
56 > These are decisions in answer to the reference
57 > monitor subject's request and allow for read, write, or
58 > execute access to system information. ;
59 > PART OF: security-control-output;
60 >
61 > INTERFACE: reference-monitor-subject;
62 > SYNONYM: rmonsub;
63 > DESCRIPTION:
64 > A reference monitor subject may be a user, a
65 > process, or a job which generates requests on the
66 > reference monitor. ;
67 > PART OF: security-control-interface;
68 > RECEIVES: reference-monitor-decision;
69 > GENERATES: reference-monitor-request;
70 >
71 > INPUT: administrative-security-command;
72 > SYNONYM: admcom;
73 > DESCRIPTION:
74 > These are commands necessary to the performance

```

## Security-control-example

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

75 > of administrative security functions and will allow for  
 76 > the maintenance of the reference monitor data base. ;

77 > ATTRIBUT: occurrences unscheduled;

78 > PART OF: security-control-input;

79 >

80 > OUTPUT: administrative-security-resp;

81 > SYNONYM: admsres;

82 > DESCRIPTION;

83 > These are responses to administrative security

84 > commands and will consist of validations as to

85 > the execution of these commands. ;

86 > PART OF: security-control-output;

87 >

88 > INTERFACE: system-security-administrator;

89 > SYNONYM: ssadm,ssa;

90 > DESCRIPTION:

91 > The system security administrator will have the  
 92 > responsibility of receiving and reviewing audit data  
 93 > contained in the auditing system data base and  
 94 > performing administrative functions dealing with the  
 95 > initiation and maintenance of system subject and object  
 96 > information contained in the reference monitor data  
 97 > base.

98 > PART OF: security-control-interface;

99 > GENERATES: administrative-security-comd;

100 > RECEIVES: administrative-security-resp;

101 > GENERATES: auditing-request;

102 > RECEIVES: audit-trail;

103 >

104 > INPUT: auditing-request;

105 > SYNONYM: audreq;

106 > DESCRIPTION;

107 > These are requests to view audit data stored in  
 108 > the auditing system data base by the reference  
 109 > monitor. ;

110 > ATTRIBUTE: occurrences scheduled;

111 > PART OF: security-control-input;

112 >

113 > OUTPUT: audit-trail;

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```

114 > SYNONYM: audtra;
115 > DESCRIPTION:
116 > Security audit trails should contain records of
117 > each security incident, and may contain other data
118 > as well. ;
119 > PART OF: security-control-output;
120 >
121 > SET: scdb;
122 > SUBSETS ARE: reference-monitor-data-base,
123 > auditing-system-data-base;
124 >
125 > SET: reference-monitor-data-base;
126 > SYNONYM: rmondb;
127 > DESCRIPTION:
128 > The information in this set consists of user access
129 > data, object sensitivity, need-to-know, etc. This
130 > information is generated by the system security
131 > administrator and users given permission. ;
132 > RESPONSIBLE-INTERFACE: system-security-administrator;
133 >
134 > SET: auditing-system-data-base;
135 > SYNONYM: audsysdb;
136 > DESCRIPTION:
137 > The system audit functions should provide a
138 > history of normal and abnormal system use, or
139 > operation, to permit regular security review of
140 > system activity. ;
141 > RESPONSIBLE-INTERFACE: system-security-administrator;
142 >
143 > DEFINE: level-2 KEYWORD;
144 > DESCRIPTION:
145 > This keyword is given to the second highest
146 > level in the scs description. ;
147 > APPLIES: rmonsub,rmonreq,rmon,rmondec,
148 > ssadm,admscom,admssys,admstres,
149 > audreq,audsys,audtra,rmondb,audsysdb;
150 >
151 > EOF

```

## DATA BASE SUMMARY

ATTRIBUTE	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE-VALUE	2	1	50.00	1	50.00
INPUT	4	0		0	
KEYWORD	4	4	100.00	4	100.00
MEMO	2	0		2	100.00
OUTPUT	1	0		1	100.00
PROCESS	4	4	100.00	4	100.00
INTERFACE	4	4	100.00	4	100.00
SET	3	3	100.00	3	100.00
	3	3	100.00	3	100.00
** TOTAL **	27	19	70.37	22	81.48

Security-control-example

PROCESS STRUCTURE

PARAMETERS FOR: STR

PROCESS INDENT=3 NOINDEX

COUNT LEVEL NAME

1	1	security-control-system
2	2	reference-monitor
3	2	administrative-security-system
4	2	auditing-system

LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT
1	1	2	3	

Security-control-example

INTERFACE STRUCTURE

PARAMETERS FOR: STR

INTERFACE INDENT=3 NOINDEX

COUNT LEVEL NAME

1	1	security-control-interface
2	2	reference-monitor-subject
3	2	system-security-administrator

LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT
1	1	2	2	

Security-control-example

INPUT STRUCTURE

PARAMETERS FOR: STR

INPUT INDENT=3 NOINDEX

COUNT LEVEL NAME

- 1 security-control-input
- 2 reference-monitor-request
- 3 administrative-security-comd
- 4 auditing-request

LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT
1	1	2	3

Security-control-example

OUTPUT STRUCTURE

PARAMETERS FOR: STR

OUTPUT INDENT=3 NOINDEX

COUNT LEVEL NAME

- 1 security-control-output
- 2 reference-monitor-decision
- 3 administrative-security-resp
- 4 audit-trail

LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT
1	1	2	3

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='SET' ORDER=BYTYPE

- |   |                             |     |
|---|-----------------------------|-----|
| 1 | auditing-system-data-base   | SET |
| 2 | reference-monitor-data-base | SET |
| 3 | security-control-data-base  | SET |

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=70 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONPW-PAGE NONPW-LINE

```

1 SET
2   SYNONYMS ARE:
3   DESCRIPTION;
4
5       The system audit functions should provide a
6       history of normal and abnormal system use, or
7       operation, to permit regular security review of
8       system activity.;
9
10  KEYWORDS:
11  SUBSET OF:
12  RESPONSIBLE-INTERFACE IS:
13
14      auditing-system-data-base;
15      audsysdb;
16
17      level-2;
18      security-control-data-base;
19      system-security-administrator;
20
21      reference-monitor-data-base;
22      rmondb;
23
24  The information in this set consists of user access
25  data, object sensitivity, need-to-know, etc. This
26  information is generated by the system security
27  administrator and users given permission.;
28
29  KEYWORDS:
30  SUBSET OF:
31  RESPONSIBLE-INTERFACE IS:
32
33      security-control-data-base;
34      scdb;
35
36  The information in this set consists of all
37  data stored and maintained by the security control
38  system.;
39
40  SPE-MEMO:
41  KEYWORDS:
42  ATTRIBUTES ARE:
43  SPECIFICATION-DERIVATION
44  SUBSETS ARE:
45
46      system-philosophy-memo;
47      level-1;
48
49      implicit;
50      reference-monitor-data-base;
51      auditing-system-data-base;
52      security-control-interface;

```

URA VERSION 3.0R1

JUN 16, 1976 00:49:28

PAGE

34

Security-control-example

FORMATTED PROBLEM STATEMENT

37 EOF EOF EOF EOF EOF

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='PROCESS' ORDER=BYTYPE

- |   |                                |         |
|---|--------------------------------|---------|
| 1 | administrative-security-system | PROCESS |
| 2 | auditing-system                | PROCESS |
| 3 | reference-monitor              | PROCESS |
| 4 | security-control-system        | PROCESS |

URA VERSION 3.0R1

Security-control-example

JUN 16, 1976 00:49:28

PAGE

36

PICTURE

PARAMETERS FOR: PIC

FILE NOINDEX DATA STRUCTURE FLOW

PROCESS PICTURE

administrative-security-system

```

+--PROCESS--+
Isecurity- I
Icontrol- I
ISystem I
+---PART-----+

```

. . . . .

```

+--PROCESS--+
Iadministra-I
Iitive-secur-I
Iity-system I
+-----+

```

```

+---INPUT---+
Iadministra-I
Iitive-secur-I
Iity-Comd I
+--RECEIVES--+

```

```

+---OUTPUT---+
Iadministra-I
Iitive-secur-I
Iity-resp I
+--GENERATES--+

```

PROCESS PICTURE

auditing-system

```

+--PROCESS--+
Isecurity-  I
Icontrol-   I
Isystem    I
+---PART---+

```

.....

```

+---INPUT---+
Iauditing-  I
Irequest    I
I           I
+--RECEIVES--+

```

```

+--PROCESS--+
Iauditing-  I
Isystem     I
I           I
+---PART---+

```

```

+---OUTPUT---+
I           I
Iaudit-trail I
I           I
+--GENERATES--+

```

PROCESS PICTURE

reference-monitor

```

+---PROCESS---+
Isecurity-  I
Icontrol-   I
Isystem    I
+---PART-----+

```

.....

```

+---INPUT---+
Ireference-  I
Imonitor-   I
Irequest    I
+---RECEIVES---+

```

```

+---PROCESS---+
Ireference-  I
Imonitor    I
I           I
+-----+

```

```

+---OUTPUT---+
Ireference-   I
Imonitor-    I
Idecision    I
+---GENERATES---+

```

PROCESS PICTURE

security-control-system

```

+---INPUT---+
Isecurity-  I
Icontrol-   I
Iinput      I
+--RECEIVES--+

```

```

+--PROCESS--+
Isecurity-   I
Icontrol-   I
Isystem     I
+-----+

```

```

+---OUTPUT---+
Isecurity-   I
Icontrol-   I
Ioutput      I
+--GENERATES--+

```

```

+--PROCESS--+ +--PROCESS--+ +--PROCESS--+
Ireference-  I Iadministra-I Iauditing-  I
Imonitor    I Iitive-secur-I Isystem   I
I           I Iity-system  I I         I
+--SUBPARTS--+ +--SUBPARTS--+ +--SUBPARTS--+

```

## Security-control-example

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYN0

SOURCE NOXREP UPDATE DBREF

LINE S T M T

ID FIELD

```

1 > /* SCS data structure */
2 >
3 > /* Reference Monitor Data Base */
4 >
5 > SET:      reference-monitor-data-base;
6 > SUBSETS:  top-secret-file,secret-file,confidential-file,
7 >            unclassified-file;
8 > SUBSETTING-CRITERIA:  sub-curr-sec-level,obj-sec-level;
9 >
10 > SET:      top-secret-file;
11 > SYNONYM:   topsecfile;
12 > DESCRIPTION;
13 >           This file contains occurrences of subject and object
14 >           information which have top secret security levels. ;
15 > CONSISTS:  subject-information, object-information;
16 >
17 > SET:      secret-file;
18 > SYNONYM:   sacfile;
19 > DESCRIPTION;
20 >           This file contains occurrences of subject and object
21 >           information which have secret security levels. ;
22 > CONSISTS:  subject-information, object-information;
23 >
24 > SET:      confidential-file;
25 > SYNONYM:   confile;
26 > DESCRIPTION;
27 >           This file contains occurrences of subject and object
28 >           information which have confidential security levels. ;
29 > CONSISTS:  subject-information, object-information;
30 >
31 > SET:      unclassified-file;
32 > SYNONYM:   uncfle;
33 > DESCRIPTION;
34 >           This file contains occurrences of subject and object
35 >           information which have unclassified security levels. ;

```

## A S - Y S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```

36 > CONSISTS: subject-information, object-information;
37 >
38 > ENTITY: subject-information;
39 > SYNONYM: subinfo;
40 > DESCRIPTION;
41 > This information holds identification and
42 > security data about a reference monitor subject. ;
43 > CONSISTS: subject-id,
44 > sub-max-sec-level,
45 > sub-curr-sec-level;
46 >
47 > ENTITY: object-information;
48 > SYNONYM: objinfo;
49 > DESCRIPTION;
50 > This information holds identification, security,
51 > and location information for a particular object. ;
52 > CONSISTS: object-id,
53 > obj-sec-level,
54 > object-location;
55 > IDENTIFIED BY: object-id;
56 >
57 > RELATION: subject-access-to-object;
58 > DESCRIPTION;
59 > This relation specifies that a subject may have
60 > usage attribute access to an object. ;
61 > BETWEEN subinfo AND objinfo;
62 > ASSOCIATED-DATA: usage-attribute;
63 >
64 > RELATION: subject-need-to-know-object;
65 > DESCRIPTION;
66 > This relation specifies that a subject has a need
67 > to know an object with usage attribute access. ;
68 > BETWEEN subinfo AND objinfo;
69 > ASSOCIATED-DATA: usage-attribute;
70 >
71 > ELEMENT: subject-id;
72 > DESCRIPTION;
73 > This is a unique identifier for a subject. ;
74 > IDENTIFIERS: subject-information;

```

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```
75 >
76 > ELEMENT: object-id;
77 > DESCRIPTION;
78 > This is a unique identifier for an object. ;
79 >
80 >
81 > ELEMENT: usage-attribute;
82 > DESCRIPTION;
83 > This specifies the type of usage, that is
84 > read, write, or execute, that a subject may have of an
85 > object. ;
86 >
87 > ELEMENT: decision-type;
88 > DESCRIPTION;
89 > This is the affirmative or negative decision to
90 > a subject's request. ;
91 >
92 >
93 > ELEMENT: requesting-subject-id,
94 > receiving-subject-id,
95 > error-code;
96 >
97 > GROUP: sub-max-sec-level;
98 > DESCRIPTION;
99 > This is the maximum security level for a subject. ;
100 > CONSISTS: classification-level,
101 > category-set;
102 >
103 > GROUP: sub-curr-sec-level;
104 > DESCRIPTION;
105 > This is the current security level for a subject. ;
106 > CONSISTS: classification-level,
107 > category-set;
108 >
109 > GROUP: obj-sec-level;
110 > DESCRIPTION;
111 > This is the security level for an object. ;
112 > CONSISTS: classification-level,
113 > category-set;
```

## A S - I S S O U R C E L I S T I N G

## LINE S T M T

ID FIELD

```

114 > ELEMENT: object-location;
115 > DESCRIPTION:
116 > This is a pointer to the actual object which
117 > contains the information of interest to a subject and
118 > which exists outside the security control system. ;
119 >
120 >
121 > ELEMENT: classification-level;
122 > DESCRIPTION:
123 > This is a level of classification which may
124 > range up from unclassified to top secret and may be
125 > owned by a subject or an object. ;
126 >
127 > ELEMENT: category-set;
128 > DESCRIPTION:
129 > This is a set of categories of information which
130 > may be owned by a subject or an object. ;
131 >
132 > /* Auditing System Data Base */
133 >
134 > ENTITY: incident-information;
135 > SYNONYM: incinfo;
136 > DESCRIPTION:
137 > This information holds data about where and
138 > when an incident has occurred. ;
139 > CONTAINED IN: audsysdb;
140 > CONSISTS: date-time,
141 > consol-nr,
142 > incident-type;
143 >
144 > RELATION: sub-inc-audit-relation;
145 > DESCRIPTION:
146 > This relates a subject to an audit incident
147 > which he has caused by trying to access objects via the
148 > reference monitor. ;
149 > BETWEEN subinfo AND incinfo;
150 >
151 > RELATION: sub-obj-audit-relation;
152 > DESCRIPTION:

```

## A S - T S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

153 > This relates a subject to an object with which  
154 > he has caused audit incidents by trying to access  
155 > the object via the reference monitor. ;  
156 > BETWEEN subinfo AND objinfo;  
157 >  
158 > RELATION: obj-inc-audit-relation;  
159 > DESCRIPTION;  
160 > This relates an object to an incident in which  
161 > subjects tried to access this object via the reference  
162 > monitor. ;  
163 > BETWEEN: objinfo AND incinfo;  
164 >  
165 > ELEMENT: incident-type;  
166 > DESCRIPTION;  
167 > This specifies the type of audit incident which  
168 > has occurred. ;  
169 >  
170 > ELEMENT: date-time;  
171 > DESCRIPTION;  
172 > This is the date and time an audit incident  
173 > occurred. ;  
174 >  
175 > ELEMENT: consol-nr;  
176 > DESCRIPTION;  
177 > This is the number of the console at which the audit  
178 > incident occurred. ;  
179 >  
180 >  
181 > ELEMENT: security-id;  
182 > DESCRIPTION;  
183 > This uniquely identifies the system security  
184 > administrator. ;  
185 >  
186 > ELEMENT: validation-code;  
187 > DESCRIPTION;  
188 > This is a validation of a command issued by  
189 > the system security administrator. ;  
190 >  
191 >

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```
192 > /* Reference Monitor Input/Output */
193 >
194 > INPUT:      get-read-request;
195 >      SYNONYM:  kf1req;
196 >      PART OP:  reference-monitor-request;
197 >      CONSISTS: subject-il,
198 >                object-id,
199 >                usage-attribute;
200 >
201 > OUTPUT:      get-read-decision;
202 >      SYNONYM:  kf1dec;
203 >      PART OP:  reference-monitor-decision;
204 >      CONSISTS: decision-type;
205 >
206 > INPUT:      get-write-request;
207 >      SYNONYM:  kf2req;
208 >      PART OP:  reference-monitor-request;
209 >      CONSISTS: subject-il,
210 >                object-id,
211 >                usage-attribute;
212 >
213 > OUTPUT:      get-write-decision;
214 >      SYNONYM:  kf2dec;
215 >      PART OP:  reference-monitor-decision;
216 >      CONSISTS: decision-type;
217 >
218 > INPUT:      get-execute-request;
219 >      SYNONYM:  kf3req;
220 >      PART OP:  reference-monitor-request;
221 >      CONSISTS: subject-il,
222 >                object-id,
223 >                usage-attribute;
224 >
225 > OUTPUT:      get-execute-decision;
226 >      SYNONYM:  kf3dec;
227 >      PART OP:  reference-monitor-decision;
228 >      CONSISTS: decision-type;
229 >
230 > INPUT:      get-read-write-request;
```

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```

231 >      SYNONYM:      kf4req;
232 >      PART OP:      reference-monitor-request;
233 >      CONSISTS:      subject-id,
234 >                     object-id,
235 >                     usage-attribute;
236 >
237 >      OUTPUT:        get-read-write-decision;
238 >      SYNONYM:        kf4dec;
239 >      PART OP:        reference-monitor-decision;
240 >      CONSISTS:        decision-type;
241 >
242 >      INPUT:          release-usage-attr-request;
243 >      SYNONYM:        kf5req;
244 >      PART OP:        reference-monitor-request;
245 >      CONSISTS:        subject-id,
246 >                     object-id,
247 >                     usage-attribute;
248 >
249 >      OUTPUT:          release-usage-attr-decision;
250 >      SYNONYM:        kf5dec;
251 >      PART OP:        reference-monitor-decision;
252 >      CONSISTS:        decision-type;
253 >
254 >      INPUT:          give-usage-attr-request;
255 >      SYNONYM:        kf6req;
256 >      PART OP:        reference-monitor-request;
257 >      CONSISTS:        requesting-subject-id,
258 >                     receiving-subject-id,
259 >                     object-id,
260 >                     usage-attribute;
261 >
262 >      OUTPUT:          give-usage-attr-decision;
263 >      SYNONYM:        kf6dec;
264 >      PART OP:        reference-monitor-decision;
265 >      CONSISTS:        decision-type;
266 >
267 >      INPUT:          rescind-usage-attr-request;
268 >      SYNONYM:        kf7req;
269 >      PART OP:        reference-monitor-request;

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```
270 > CONSISTS: requesting-subject-id,  
271 > receiving-subject-id,  
272 > object-id,  
273 > usage-attribute;  
274 >  
275 > OUTPUT: rescind-usage-attr-decision;  
276 > SYNONYM: kf7dec;  
277 > PART OF: reference-monitor-decision;  
278 > CONSISTS: decision-type;  
279 >  
280 > INPUT: create-object-request;  
281 > SYNONYM: kf8req;  
282 > PART OF: reference-monitor-request;  
283 > CONSISTS: subject-id,  
284 > object-id,  
285 > obj-sec-level;  
286 >  
287 > OUTPUT: create-object-decision;  
288 > SYNONYM: kf8dec;  
289 > PART OF: reference-monitor-decision;  
290 > CONSISTS: decision-type;  
291 >  
292 > INPUT: delete-object-request;  
293 > SYNONYM: kf9req;  
294 > PART OF: reference-monitor-request;  
295 > CONSISTS: subject-id,  
296 > object-id;  
297 >  
298 > OUTPUT: delete-object-decision;  
299 > SYNONYM: kf9dec;  
300 > PART OF: reference-monitor-decision;  
301 > CONSISTS: decision-type;  
302 >  
303 > INPUT: change-sub-curr-sec-level-req;  
304 > SYNONYM: kf10req;  
305 > PART OF: reference-monitor-request;  
306 > CONSISTS: subject-id,  
307 > sub-curr-sec-level;  
308 >
```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```

309 > OUTPUT: change-sub-curr-sec-level-dec;
310 > SYNONYM: kf10dec;
311 > PART OF: reference-monitor-decision;
312 > CONSISTS: decision-type;
313 >
314 > INPUT: change-obj-sec-level-request;
315 > SYNONYM: kf11req;
316 > PART OF: reference-monitor-request;
317 > CONSISTS: subject-id,
318 > object-id,
319 > obj-sec-level;
320 >
321 > OUTPUT: change-obj-sec-level-decision;
322 > SYNONYM: kf11dec;
323 > PART OF: reference-monitor-decision;
324 > CONSISTS: decision-type;
325 >
326 > /* Administrative Security System Input/Output */
327 >
328 > INPUT: create-subject-command;
329 > SYNONYM: cresubcom;
330 > PART OF: admscom;
331 > CONSISTS: security-id,
332 > subject-id,
333 > sub-max-sec-level,
334 > sub-curr-sec-level;
335 >
336 > OUTPUT: create-subject-response;
337 > SYNONYM: cresubres;
338 > PART OF: admsres;
339 > CONSISTS: validation-code;
340 >
341 > INPUT: delete-subject-command;
342 > SYNONYM: delsubcom;
343 > PART OF: admscom;
344 > CONSISTS: security-id,
345 > subject-id;
346 >
347 > OUTPUT: delete-subject-response;

```

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```

348 >      SYNONYM:  falsubres;
349 >      PART OF:  admsres;
350 >      CONSISTS: validation-code;
351 >
352 >      INPUT:    change-sub-max-sec-level-comd;
353 >      SYNONYM:  chasubmaxseclevcom;
354 >      PART OF:  admscom;
355 >      CONSISTS: security-id,
356 >               subject-id,
357 >               sub-max-sec-level;
358 >
359 >      OUTPUT:   change-sub-max-sec-level-resp;
360 >      SYNONYM:  chasubmaxseclevres;
361 >      PART OF:  admsres;
362 >      CONSISTS: validation-code;
363 >
364 >      INPUT:    link-reference-monitor-comd;
365 >      SYNONYM:  linrmncom;
366 >      PART OF:  admscom;
367 >      CONSISTS: security-id;
368 >
369 >      OUTPUT:   link-reference-monitor-resp;
370 >      SYNONYM:  linrmnres;
371 >      PART OF:  admsres;
372 >      CONSISTS: validation-code;
373 >
374 >      /* Auditing System Input/Output */
375 >
376 >      INPUT:    sub-obj-audit-request;
377 >      SYNONYM:  sibobjaudreq;
378 >      PART OF:  audreq;
379 >      CONSISTS: subject-id,
380 >               object-id;
381 >
382 >      OUTPUT:   sub-obj-audit-trail;
383 >      SYNONYM:  sibobjaudtra;
384 >      PART OF:  audtra;
385 >      CONSISTS: inc-audit-information;
386 >

```

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```
387 > GROUP: inc-audit-information;
388 > SYNONYM: incaudinfo;
389 > CONSISTS: incident-type,
390 > date-time,
391 > consol-nr;
392 >
393 > INPUT: sub-inc-audit-request;
394 > SYNONYM: subincaudreq;
395 > PART OF: audreq;
396 > CONSISTS: subject-id,
397 > incident-type;
398 >
399 > OUTPUT: sub-inc-audit-trail;
400 > SYNONYM: subincaudtra;
401 > PART OF: audtra;
402 > CONSISTS: obj-audit-information;
403 >
404 > GROUP: obj-audit-information;
405 > SYNONYM: objaudinfo;
406 > CONSISTS: object-id,
407 > date-time,
408 > consol-nr;
409 >
410 > INPUT: sub-obj-inc-audit-request;
411 > SYNONYM: subobjircaudreq;
412 > PART OF: audreq;
413 > CONSISTS: subject-id,
414 > object-id,
415 > incident-type;
416 >
417 > OUTPUT: sub-obj-inc-audit-trail;
418 > SYNONYM: subobjincaudtra;
419 > PART OF: audtra;
420 > CONSISTS: audit-information;
421 >
422 > GROUP: audit-information;
423 > SYNONYM: audinfo;
424 > CONSISTS: date-time,
425 > consol-nr;
```

## A S - I S S O U R C E L I S T I N G

## LINE S T M T

## ID FIELD

```
426 > INPUT: sub-audit-request;
427 > SYNONYM: subaudreq;
428 > PART OP: audreq;
429 > CONSISTS: subject-id;
430 >
431 > OUTPUT: sub-audit-trail;
432 > SYNONYM: subaudtra;
433 > PART OP: audtra;
434 > CONSISTS: obj-inc-audit-information;
435 >
436 >
437 > GROUP: obj-inc-audit-information;
438 > SYNONYM: objincaudinfo;
439 > CONSISTS: object-id,
440 > incident-type,
441 > date-time,
442 > consol-nr;
443 >
444 > INPUT: obj-inc-audit-request;
445 > SYNONYM: objincaudreq;
446 > PART OP: audreq;
447 > CONSISTS: object-id,
448 > incident-type;
449 >
450 > OUTPUT: obj-inc-audit-trail;
451 > SYNONYM: objincaudtra;
452 > PART OP: audtra;
453 > CONSISTS: sub-audit-information;
454 >
455 > GROUP: sub-audit-information;
456 > SYNONYM: subaudinfo;
457 > CONSISTS: subject-id,
458 > date-time,
459 > consol-nr;
460 >
461 > INPUT: obj-audit-request;
462 > SYNONYM: objaudreq;
463 > PART OP: audreq;
464 > CONSISTS: object-id;
```

A S - I S S O U R C E L I S T I N G

CONFIDENTIAL

ID FIELD

```

4865 > OUTPUT:  obj-audit-trail;
4866 > SYNONYM:  objaudtra;
4867 > PART OF:  audtra;
4868 > CONSISTS:  sub-inc-audit-information;
4869 >
4870 >
4871 > GROUP:  sub-inc-audit-information;
4872 > SYNONYM:  subincaudinfor;
4873 > CONSISTS:  subject-id,
4874 >             incident-type,
4875 >             date-time,
4876 >             consol-nr;
4877 >
4878 >
4879 > INPUT:  inc-audit-request;
4880 > SYNONYM:  incaudreq;
4881 > PART OF:  audreq;
4882 > CONSISTS:  incident-type;
4883 >
4884 >
4885 > OUTPUT:  inc-audit-trail;
4886 > SYNONYM:  incaudtra;
4887 > PART OF:  audtra;
4888 > CONSISTS:  sub-obj-audit-information;
4889 >
4890 >
4891 > GROUP:  sub-obj-audit-information;
4892 > SYNONYM:  subobjaudinfo;
4893 > CONSISTS:  subject-id,
4894 >             object-id,
4895 >             date-time,
4896 >             consol-nr;
4897 >
4898 >
4899 > INPUT:  dump-audit-request;
4900 > SYNONYM:  dumaudreq;
4901 > PART OF:  audreq;
4902 >
4903 >
4904 > OUTPUT:  dump-audit-trail;
4905 > SYNONYM:  dumaudtra;
4906 > PART OF:  audtra;
4907 > CONSISTS:  sub-obj-inc-audit-information;
4908 >
4909 >
4910 >
4911 >
4912 >
4913 >
4914 >
4915 >
4916 >
4917 >
4918 >
4919 >
4920 >
4921 >
4922 >
4923 >
4924 >
4925 >
4926 >
4927 >
4928 >
4929 >
4930 >
4931 >
4932 >
4933 >
4934 >
4935 >
4936 >
4937 >
4938 >
4939 >
4940 >
4941 >
4942 >
4943 >
4944 >
4945 >
4946 >
4947 >
4948 >
4949 >
4950 >
4951 >
4952 >
4953 >

```

A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

504 > GROUP: sub-obj-inc-audit-information;  
 505 > SYNONYM: sibobjincautinfo;  
 506 > CONSISTS: subject-id,  
 507 > object-id,  
 508 > incident-type,  
 509 > date-time,  
 510 > consol-nr;  
 511 >  
 512 >

EOF

## Security-control-example

## DATA BASE SUMMARY

ATTRIBUTE	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE-VALUE	2	1	50.00	1	50.00
ELEMENT	4	0		0	
ENTITY	15	0		12	80.00
GROUP	3	3	100.00	3	100.00
INPUT	11	8	72.73	3	27.27
KEYWORD	27	27	100.00	4	14.81
MEMO	2	0		2	100.00
OUTPUT	1	0		1	100.00
PROCESS	27	27	100.00	4	14.81
INTERFACE	4	4	100.00	4	100.00
RELATION	3	3	100.00	3	100.00
SET	5	0		5	100.00
	7	7	100.00	7	100.00
** TOTAL **	111	80	72.07	49	44.14

## Security-control-example

## Name Generation

## PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='OUT' ORDER=BYTYPE

1	administrative-security-resp	OUTPUT
2	audit-trail	OUTPUT
3	change-obj-sec-level-decision	OUTPUT
4	change-sub-curr-sec-level-dec	OUTPUT
5	change-sub-max-sec-level-resp	OUTPUT
6	create-object-decision	OUTPUT
7	create-subject-response	OUTPUT
8	delete-object-decision	OUTPUT
9	delete-subject-response	OUTPUT
10	dump-audit-trail	OUTPUT
11	get-execute-decision	OUTPUT
12	get-read-decision	OUTPUT
13	get-read-write-decision	OUTPUT
14	get-write-decision	OUTPUT
15	give-usage-attr-decision	OUTPUT
16	inc-audit-trail	OUTPUT
17	link-reference-monitor-resp	OUTPUT
18	obj-audit-trail	OUTPUT
19	obj-inc-audit-trail	OUTPUT
20	reference-monitor-decision	OUTPUT
21	release-usage-attr-decision	OUTPUT
22	rescind-usage-attr-decision	OUTPUT
23	security-control-output	OUTPUT
24	sub-audit-trail	OUTPUT
25	sub-inc-audit-trail	OUTPUT
26	sub-obj-audit-trail	OUTPUT
27	sub-obj-inc-audit-trail	OUTPUT

## Security-control-example

## CONTENTS REPORT

## PARAMETERS FOR: CONT

FILE NONCPLAG INDEX LEVELS=ALL

- 1\* 1 administrative-security-resp (OUTPUT)
- 2\* 1 audit-trail (OUTPUT)
- 3\* 1 change-obj-sec-level-decision (OUTPUT)
  - 2 decision-type (ELEMENT)
- 4\* 1 change-sub-curr-sec-level-dec (OUTPUT)
  - 2 decision-type (ELEMENT)
- 5\* 1 change-sub-max-sec-level-tesp (OUTPUT)
  - 2 validation-code (ELEMENT)
- 6\* 1 create-object-decision (OUTPUT)
  - 2 decision-type (ELEMENT)
- 7\* 1 create-subject-response (OUTPUT)
  - 2 validation-code (ELEMENT)
- 8\* 1 delete-object-decision (OUTPUT)
  - 2 decision-type (ELEMENT)
- 9\* 1 delete-subject-response (OUTPUT)
  - 2 validation-code (ELEMENT)
- 10\* 1 dump-audit-trail (OUTPUT)
  - 2 sub-obj-inc-audit-information (GROUP)
    - 3 subject-id (ELEMENT)
    - 3 object-id (ELEMENT)
    - 3 incident-type (ELEMENT)
    - 3 date-time (ELEMENT)
    - 3 consol-nr (ELEMENT)
- 11\* 1 get-execute-decision (OUTPUT)
  - 2 decision-type (ELEMENT)

## Security-control-example

## CONTENTS REPORT

12*	1	1	get-read-decision (OUTPUT)
	2	1	decision-type (ELEMENT)
13*	1	1	1 get-read-write-decision (OUTPUT)
	2	1	decision-type (ELEMENT)
14*	1	1	1 get-write-decision (OUTPUT)
	2	1	decision-type (ELEMENT)
15*	1	1	1 give-usage-attr-decision (OUTPUT)
	2	1	decision-type (ELEMENT)
16*	1	1	1 inc-audit-trail (OUTPUT)
	2	1	sub-obj-audit-information (GROUP)
	3	1	subject-id (ELEMENT)
	3	1	object-id (ELEMENT)
	3	1	date-time (ELEMENT)
	3	1	consol-nr (ELEMENT)
17*	1	1	1 link-reference-monitor-resp (OUTPUT)
	2	1	validation-code (ELEMENT)
18*	1	1	1 obj-audit-trail (OUTPUT)
	2	1	sub-inc-audit-information (GROUP)
	3	1	subject-id (ELEMENT)
	3	1	incident-type (ELEMENT)
	3	1	date-time (ELEMENT)
	3	1	consol-nr (ELEMENT)
19*	1	1	1 obj-inc-audit-trail (OUTPUT)
	2	1	sub-audit-information (GROUP)
	3	1	subject-id (ELEMENT)
	3	1	date-time (ELEMENT)
	3	1	consol-nr (ELEMENT)
20*	1	1	1 reference-monitor-decision (OUTPUT)
21*	1	1	1 release-usage-attr-decision (OUTPUT)
	2	1	decision-type (ELEMENT)
22*	1	1	1 rescind-usage-attr-decision (OUTPUT)

## Security-control-example

## CONTENTS REPORT

1	2	decision-type (ELEMENT)
23*	1	security-control-output (OUTPUT)
24*	1	sub-audit-trail (OUTPUT)
1	2	obj-inc-audit-information (GROUP)
2	3	object-id (ELEMENT)
3	3	incident-type (ELEMENT)
4	3	date-time (ELEMENT)
5	3	consol-nr (ELEMENT)
25*	1	sub-inc-audit-trail (OUTPUT)
1	2	obj-audit-information (GROUP)
2	3	object-id (ELEMENT)
3	3	date-time (ELEMENT)
4	3	consol-nr (ELEMENT)
26*	1	sub-obj-audit-trail (OUTPUT)
1	2	inc-audit-information (GROUP)
2	3	incident-type (ELEMENT)
3	3	date-time (ELEMENT)
4	3	consol-nr (ELEMENT)
27*	1	sub-obj-inc-audit-trail (OUTPUT)
1	2	audit-information (GROUP)
2	3	date-time (ELEMENT)
3	3	consol-nr (ELEMENT)

## Security-control-example

## INDEX

1 administrative-security-resp	57
2 audit-information	59
3 audit-trail	57
4 change-obj-sec-level-decision	57
5 change-sub-curr-sec-level-dec	57
6 change-sub-max-sec-level-resp	57
7 consol-nr	57, 58( 3), 59( 4)
8 create-object-decision	57
9 create-subject-response	57
10 date-time	57, 58( 3), 59( 4)
11 decision-type	57( 5), 58( 5), 59
12 delete-object-decision	57
13 delete-subject-response	57
14 dump-audit-trail	57
15 get-execute-decision	57
16 get-read-decision	58
17 get-read-write-decision	58
18 get-write-decision	58
19 give-usage-attr-decision	58
20 inc-audit-information	59
21 inc-audit-trail	58

## Security-control-example

## INDEX

22 incident-type	57, 58, 59( 2)
23 link-reference-monitor-resp	58
24 obj-audit-information	59
25 obj-audit-trail	58
26 obj-inc-audit-information	59
27 obj-inc-audit-trail	58
28 object-id	57, 58, 59( 2)
29 reference-monitor-decision	58
30 release-usage-attr-decision	58
31 rescind-usage-attr-decision	58
32 security-control-output	59
33 sub-audit-information	58
34 sub-audit-trail	59
35 sub-inc-audit-information	58
36 sub-inc-audit-trail	59
37 sub-obj-audit-information	58
38 sub-obj-audit-trail	59
39 sub-obj-inc-audit-information	57
40 sub-obj-inc-audit-trail	59
41 subject-id	57, 58( 3)
42 validation-code	57( 3), 58

## Security-control-example

## Name Generation

## PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='INP' ORDER=BYTYPE

1	administrative-security-comd	INPUT
2	auditing-request	INPUT
3	change-obj-sec-level-request	INPUT
4	change-sub-curr-sec-level-req	INPUT
5	change-sub-max-sec-level-comd	INPUT
6	create-object-request	INPUT
7	create-subject-command	INPUT
8	delete-object-request	INPUT
9	delete-subject-command	INPUT
10	dump-audit-request	INPUT
11	get-execute-request	INPUT
12	get-read-request	INPUT
13	get-read-write-request	INPUT
14	get-write-request	INPUT
15	give-usage-attr-request	INPUT
16	inc-audit-request	INPUT
17	link-reference-monitor-comd	INPUT
18	obj-audit-request	INPUT
19	obj-inc-audit-request	INPUT
20	reference-monitor-request	INPUT
21	release-usage-attr-request	INPUT
22	rescind-usage-attr-request	INPUT
23	security-control-input	INPUT
24	sub-audit-request	INPUT
25	sub-inc-audit-request	INPUT
26	sub-obj-audit-request	INPUT
27	sub-obj-inc-audit-request	INPUT

CONSISTS COMPARISON REPORT

PARAMETERS FOR: CNC

FILE

URA273:CNCBLD	:	NAME	DOESNT	CONSIST	OF	ANYTHING	-	administrative-security-cond
URA273:CNCBLD	:	NAME	DOESNT	CONSIST	OF	ANYTHING	-	auditing-request
URA273:CNCBLD	:	NAME	DOESNT	CONSIST	OF	ANYTHING	-	dump-audit-request
URA273:CNCBLD	:	NAME	DOESNT	CONSIST	OF	ANYTHING	-	reference-monitor-request
URA273:CNCBLD	:	NAME	DOESNT	CONSIST	OF	ANYTHING	-	security-control-input

## CONSISTS COMPARISON REPORT

## BASIC CONTENTS MATRIX

The rows are the given input names.

The columns are the lowest level objects which are contained in the rows, with intermediate groups ignored.

If any columns are group names, then the definition is incomplete.

If any columns are ambiguous names, they are possible elements.

## ROW NAMES

1	change-obj-sec-level-request	INPUT
2	change-sub-curr-sec-level-req	INPUT
3	change-sub-max-sec-level-comd	INPUT
4	create-object-request	INPUT
5	create-subject-command	INPUT
6	delete-object-request	INPUT
7	delete-subject-command	INPUT
8	get-execute-request	INPUT
9	get-read-request	INPUT
10	get-read-write-request	INPUT
11	get-write-request	INPUT
12	give-usage-attr-request	INPUT
13	inc-audit-request	INPUT
14	link-reference-monitor-comd	INPUT
15	obj-audit-request	INPUT
16	obj-inc-audit-request	INPUT
17	release-usage-attr-request	INPUT
18	rescind-usage-attr-request	INPUT
19	sub-audit-request	INPUT
20	sub-inc-audit-request	INPUT
21	sub-obj-audit-request	INPUT
22	sub-obj-inc-audit-request	INPUT

## COLUMN NAMES

1	subject-id	ELEMENT
2	object-id	ELEMENT
3	classification-level	ELEMENT
4	category-set	ELEMENT
5	security-id	ELEMENT
6	usage-attribute	ELEMENT
7	requesting-subject-id	ELEMENT
8	receiving-subject-id	ELEMENT
9	incident-type	ELEMENT

Security-control-example

CONSISTS COMPARISON REPORT

## BASIC CONTENTS MATRIX

An \* in (i,j) means that column j is contained directly or indirectly in row i. The columns do not consist of anything further. Intermediate groups are ignored.

```

123456789
+-----+
1 I****
2 I* **
3 I* ***
4 I*****
5 I* ****
+-----+
6 I**
7 I* *
8 I** *
9 I** *
10 I** *
+-----+
11 I** *
12 I* ***
13 I *
14 I *
15 I *
+-----+
16 I* *
17 I** *
18 I* ***
19 I*
20 I* *
+-----+
21 I**
22 I** *
+-----+

```

## Security-control-example

## CONSISTS COMPARISON REPORT

## CONTENTS SIMILARITY SUMMARY

ROW#	NAME	IS A SUBSET OF	IS EQUIVALENT TO	ROW#	NAME
2	change-sub-curr-sec-level-req			1	change-obj-sec-level-request
1	change-obj-sec-level-request			4	create-object-request
6	delete-object-request	IS A SUBSET OF	IS EQUIVALENT TO	1	change-obj-sec-level-request
15	obj-audit-request	IS A SUBSET OF		1	change-obj-sec-level-request
19	sub-audit-request	IS A SUBSET OF		1	change-obj-sec-level-request
21	sub-obj-audit-request	IS A SUBSET OF		1	change-obj-sec-level-request
2	change-sub-curr-sec-level-req	IS A SUBSET OF		1	change-obj-sec-level-request
2	change-sub-curr-sec-level-req	IS A SUBSET OF		3	change-sub-max-sec-level-command
2	change-sub-curr-sec-level-req	IS A SUBSET OF		4	create-object-request
19	sub-audit-request	IS A SUBSET OF		5	create-subject-command
3	change-sub-max-sec-level-command	IS A SUBSET OF	IS EQUIVALENT TO	2	change-sub-curr-sec-level-request
7	delete-subject-command	IS A SUBSET OF		5	create-subject-command
14	link-reference-monitor-command	IS A SUBSET OF		3	change-sub-max-sec-level-command
19	sub-audit-request	IS A SUBSET OF		3	change-sub-max-sec-level-command
6	delete-object-request	IS A SUBSET OF		4	create-object-request
15	obj-audit-request	IS A SUBSET OF		4	create-object-request
19	sub-audit-request	IS A SUBSET OF		4	create-object-request
21	sub-obj-audit-request	IS A SUBSET OF		4	create-object-request
7	delete-subject-command	IS A SUBSET OF		5	create-subject-command
14	link-reference-monitor-command	IS A SUBSET OF		5	create-subject-command
19	sub-audit-request	IS A SUBSET OF		5	create-subject-command
6	delete-object-request	IS A SUBSET OF		8	get-execute-request
6	delete-object-request	IS A SUBSET OF		9	get-read-request
6	delete-object-request	IS A SUBSET OF		10	get-read-write-request
6	delete-object-request	IS A SUBSET OF		11	get-write-request
15	obj-audit-request	IS A SUBSET OF		6	delete-object-request
6	delete-object-request	IS A SUBSET OF		17	release-usage-attr-request
19	sub-audit-request	IS A SUBSET OF		6	delete-object-request
6	delete-object-request	IS A SUBSET OF		21	sub-obj-audit-request
6	delete-object-request	IS A SUBSET OF	IS EQUIVALENT TO	22	sub-obj-inc-audit-request
14	link-reference-monitor-command	IS A SUBSET OF		7	delete-subject-command
19	sub-audit-request	IS A SUBSET OF		7	delete-subject-command
8	get-execute-request	IS EQUIVALENT TO		9	get-read-request
8	get-execute-request	IS EQUIVALENT TO		10	get-read-write-request
8	get-execute-request	IS EQUIVALENT TO		11	get-write-request
15	obj-audit-request	IS A SUBSET OF		8	get-execute-request
8	get-execute-request	IS EQUIVALENT TO		17	release-usage-attr-request

AD-A065 948

MICHIGAN UNIV ANN ARBOR DEPT OF INDUSTRIAL AND OPERA--ETC F/G 5/9  
URL/URA TRAINING EXAMPLE.(U)  
DEC 78

UNCLASSIFIED

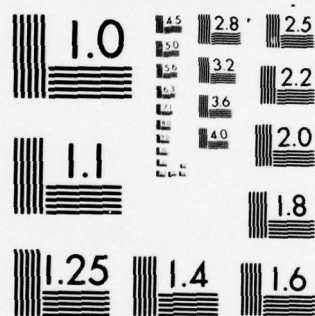
ESD-TR-78-126

F19628-76-C-0197  
NL

2 OF 3

AD  
A06594





MICROCOPY RESOLUTION TEST CHART  
NATIONAL BUREAU OF STANDARDS-1963-A

CONSISTS COMPARISON REPORT

CONTENT'S SIMILARITY SUMMARY

ROW#	NAME	ROW#	NAME
19	sub-audit-request	8	get-execute-request
21	sub-obj-audit-request	8	get-execute-request
9	get-read-request	10	get-read-write-request
9	get-read-request	11	get-write-request
15	obj-audit-request	9	get-read-request
9	get-read-request	17	release-usage-attr-request
19	sub-audit-request	9	get-read-request
21	sub-obj-audit-request	9	get-read-request
10	get-read-write-request	11	get-write-request
15	obj-audit-request	10	get-read-write-request
10	get-read-write-request	17	release-usage-attr-request
19	sub-audit-request	10	get-read-write-request
21	sub-obj-audit-request	10	get-read-write-request
15	obj-audit-request	11	get-write-request
11	get-write-request	17	release-usage-attr-request
19	sub-audit-request	11	get-write-request
21	sub-obj-audit-request	11	get-write-request
15	obj-audit-request	12	give-usage-attr-request
12	give-usage-attr-request	18	rescind-usage-attr-request
13	inc-audit-request	16	obj-inc-audit-request
13	inc-audit-request	20	sub-inc-audit-request
13	inc-audit-request	22	sub-obj-inc-audit-request
15	obj-audit-request	16	obj-inc-audit-request
15	obj-audit-request	17	release-usage-attr-request
15	obj-audit-request	18	rescind-usage-attr-request
15	obj-audit-request	21	sub-obj-audit-request
15	obj-audit-request	22	sub-obj-inc-audit-request
16	obj-inc-audit-request	22	sub-obj-inc-audit-request
19	sub-audit-request	17	release-usage-attr-request
21	sub-obj-audit-request	17	release-usage-attr-request
19	sub-audit-request	20	sub-inc-audit-request
19	sub-audit-request	21	sub-obj-audit-request
19	sub-audit-request	22	sub-obj-inc-audit-request
20	sub-inc-audit-request	22	sub-obj-inc-audit-request
21	sub-obj-audit-request	22	sub-obj-inc-audit-request

URA VERSION 3.0R1

JUN 16, 1976 00:49:28

PAGE

69

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ENTITY' ORDER=BYTYPE

1	incident-information	ENTITY
2	object-information	ENTITY
3	subject-information	ENTITY

Security-control-example

IDENTIFIER INFORMATION REPORT

PARAMETERS FOR: EI

FILE ENTITY

URA308:IDENTC : THE FOLLOWING NAMES ARE NOT IDENTIFIED BY ANYTHING:  
incident-information

ROW NAMES

1 object-id  
2 subject-id

COLUMN NAMES

ELEMENT  
ELEMENT

1 object-information  
2 subject-information

ENTITY  
ENTITY

THE ROWS ARE IDENTIFIERS OF THE COLUMNS WITH \*S

12

+--+  
1 I\* I  
2 I \*I  
+--+

IDENTIFIER INFORMATION REPORT

\*\*THE NUMBER OF COLUMNS IDENTIFIED BY THE ROWS\*\*

ROW	TYPE	COUNT
1 object-id	ELEMENT	1
2 subject-id	ELEMENT	1

\*\*THE NUMBER OF ROWS THAT IDENTIFY THE COLUMNS\*\*

COLUMN	TYPE	COUNT
1 object-information	ENTITY	1
2 subject-information	ENTITY	1

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='RELATION' ORDER=BYTYPE

- 1 obj-inc-audit-relation
- 2 sub-inc-audit-relation
- 3 sub-obj-audit-relation
- 4 subject-access-to-object
- 5 subject-need-to-know-object

RELATION  
RELATION  
RELATION  
RELATION  
RELATION

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 PMARG=70 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```

1 RELATION                                obj-inc-audit-relation;
2 DESCRIPTION;
3                                     This relates an object to an incident in which
4 subjects tried to access this object via the reference
5 monitor.;
6 BETWEEN:
7   object-information AND              incident-information;
8
9 RELATION                                sub-inc-audit-relation;
10 DESCRIPTION;
11                                     This relates a subject to an audit incident
12 which he has caused by trying to access objects via the .
13 reference monitor.;
14 BETWEEN:
15   subject-information AND            incident-information;
16
17 RELATION                                sub-obj-audit-relation;
18 DESCRIPTION;
19                                     This relates a subject to an object with which
20 he has caused audit incidents by trying to access
21 the object via the reference monitor.;
22 BETWEEN:
23   subject-information AND            object-information;
24
25 RELATION                                subject-access-to-object;
26 DESCRIPTION;
27                                     This relation specifies that a subject may have
28 usage attribute access to an object.;
29 ASSOCIATED-DATA IS:
30   BETWEEN:
31     subject-information AND          object-information;
32
33 RELATION                                subject-need-to-know-object;
34 DESCRIPTION;
35                                     This relation specifies that a subject has a need
36 to know an object with usage attribute access.;

```

URA VERSION 3.0R1

JUN 16, 1976 00:49:28

PAGE

74

Security-control-example

FORMATTED PROBLEM STATEMENT

37 ASSOCIATED-DATA IS:  
38 BETWEEN:  
39 subject-information AND  
40 object-information;  
41 EOF EOF EOF EOF EOF

usage-attribute;

## A S - I S   S O U R C E   L I S T I N G

PARAMETERS POP: SYN0

SOURCE NOXREF UPDATE DBREF

LINE S T M T

ID FIELD

```

1 > /* SCS data derivation */
2 >
3 > PROCESS: reference-monitor;
4 > USFS: reference-monitor-request;
5 > DERIVES: reference-monitor-decision;
6 > USFS: reference-monitor-data-base;
7 > UPDATES: auditing-system-data-base;
8 >
9 > PROCESS: administrative-security-system;
10 > USFS: administrative-security-comd;
11 > DERIVES: administrative-security-resp;
12 > UPDATES: reference-monitor-data-base;
13 >
14 > PROCESS: auditing-system;
15 > USFS: auditing-request;
16 > DERIVES: audit-trail;
17 > USFS: auditing-system-data-base;
18 >
19 > /* Reference Monitor Functions */
20 >
21 > PROCESS: get-read;
22 > SYNONYM: kf1;
23 > DESCRIPTION:
24 > This process decides whether or not to enable
25 > subject with subject-id read only access to object with
26 > object-id.
27 > PART OF: reference-monitor;
28 > USFS: get-read-request;
29 > DERIVES: get-read-decision;
30 >
31 > PROCESS: get-write;
32 > SYNONYM: kf2;
33 > DESCRIPTION:
34 > This process decides whether or not to enable
35 > subject with subject-id write only access to object

```

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```

36 > with object-id.
37 > PART OP: reference-monitor;
38 > USES: get-write-request;
39 > DERIVES: get-write-decision;
40 >
41 > PROCESS: get-execute;
42 > SYNONYM: kf3;
43 > DESCRIPTION;
44 > This process decides whether or not to enable
45 > subject with subject-id execute access to object with
46 > object-id. This process is only useful if the
47 > object-id requested is a procedure. ;
48 > PART OP: reference-monitor;
49 > USES: get-execute-request;
50 > DERIVES: get-execute-decision;
51 >
52 > PROCESS: get-read-write;
53 > SYNONYM: kf4;
54 > DESCRIPTION;
55 > This process decides whether or not to enable
56 > subject with subject-id read and write access to object
57 > with object-id. ;
58 > PART OP: reference-monitor;
59 > USES: get-read-write-request;
60 > DERIVES: get-read-write-decision;
61 >
62 > PROCESS: release-usage-attr;
63 > SYNONYM: kf5;
64 > DESCRIPTION;
65 > This process releases usage attribute access
66 > to object with object-id from subject with subject-id.;
67 > PART OP: reference-monitor;
68 > USES: release-usage-attr-request;
69 > DERIVES: release-usage-attr-decision;
70 >
71 > PROCESS: give-usage-attr;
72 > SYNONYM: kf6;
73 > DESCRIPTION;
74 > This process decides whether or not subject with

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

75 > requesting-subject-id may give subject with  
 76 > receiving-subject-id usage attribute access to object  
 77 > with object-id. ;

78 > PART OF: reference-monitor;  
 79 > USES: give-usage-attr-request;  
 80 > DERIVES: give-usage-attr-decision;  
 81 >

82 > PROCESS: rescind-usage-attr;  
 83 > SYNONYM: kf7;  
 84 > DESCRIPTION;

85 > This process decides whether or not subject  
 86 > with requesting-subject-id may take usage attribute  
 87 > access of object with object-id from subject with  
 88 > receiving-subject-id. ;

89 > PART OF: reference-monitor;  
 90 > USES: rescind-usage-attr-request;  
 91 > DERIVES: rescind-usage-attr-decision;  
 92 >

93 > PROCESS: create-object;  
 94 > SYNONYM: kf8;  
 95 > DESCRIPTION;

96 > This process decides whether or not subject with  
 97 > subject-id may add an object to the directory  
 98 > hierarchy directly below directory object with  
 99 > object-id. This added object is requested to have  
 100 > security level obj-sec-level. ;

101 > PART OF: reference-monitor;  
 102 > USES: create-object-request;  
 103 > DERIVES: create-object-decision;  
 104 >

105 > PROCESS: delete-object;  
 106 > SYNONYM: kf9;  
 107 > DESCRIPTION;

108 > This process decides whether or not subject with  
 109 > subject-id may delete an object with object-id from the  
 110 > appropriate set in the reference monitor data base. ;

111 > PART OF: reference-monitor;  
 112 > USES: delete-object-request;  
 113 > DERIVES: delete-object-decision;

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```

114 >
115 > PROCESS: change-sub-curr-sec-level;
116 > SYNONYM: kf10;
117 > DESCRIPTION;
118 > This process decides whether or not subject with
119 > subject-id may change his current security level to
120 > sub-curr-sec-level.
121 > PART OF: reference-monitor;
122 > USES: change-sub-curr-sec-level-req;
123 > DERIVES: change-sub-curr-sec-level-dec;
124 >
125 > PROCESS: change-obj-sec-level;
126 > SYNONYM: kf11;
127 > DESCRIPTION;
128 > This process decides whether or not subject with
129 > subject-id may revise the security level of object
130 > with object-id to the value of obj-sec-level.
131 > PART OF: reference-monitor;
132 > USES: change-obj-sec-level-request;
133 > DERIVES: change-obj-sec-level-decision;
134 >
135 > /* Administrative Security System Functions */
136 >
137 > PROCESS: create-subject;
138 > SYNONYM: cresub;
139 > DESCRIPTION;
140 > This process allows the system security
141 > administrator with security-id to create the record
142 > of a subject with subject-id. This subject will
143 > be assigned maximum security level sub-max-sec-level and
144 > current security level obj-sec-level.
145 > PART OF: admssys;
146 > USES: create-subject-command;
147 > DERIVES: create-subject-response;
148 >
149 > PROCESS: delete-subject;
150 > SYNONYM: delsub;
151 > DESCRIPTION;
152 > This process allows the system security

```

## A S - I S S O U R C E L I S T I N G

## LINE S T M T

## ID FIELD

```

153 > administrator with security-id to delete the record
154 > of a subject with subject-id.
155 > PART OF: admssys;
156 > USES: delete-subject-command;
157 > DERIVES: delete-subject-response;
158 >
159 > PROCESS: change-sub-max-sec-level;
160 > SYNONYM: chasubmaxseclv;
161 > DESCRIPTION:
162 > This process allows the system security
163 > administrator with security-id to change the maximum
164 > security level of subject with subject-id to
165 > sub-max-sec-level.
166 >
167 > PART OF: admssys;
168 > USES: change-sub-max-sec-level-com1;
169 > DERIVES: change-sub-max-sec-level-resp;
170 >
171 > PROCESS: link-reference-monitor;
172 > SYNONYM: linkrmon;
173 > DESCRIPTION:
174 > This process allows the system security
175 > administrator with security-id to perform all
176 > reference monitor functions without security checks
177 > by the reference monitor. He may perform these
178 > functions for any subject-id registered in the system.
179 > This process will effectively link the administrative
180 > security system to the reference monitor with the only
181 > security check being that of the system security
182 > administrator's security-id.
183 > PART OF: admssys;
184 > USES: link-reference-monitor-com1;
185 > DERIVES: link-reference-monitor-resp;
186 >
187 > /* Auditing System Functions */
188 >
189 > PROCESS: sub-obj-audit;
190 > SYNONYM: subobjaud;
191 > DESCRIPTION:
192 > This process allows the system security

```

## A S - I S S O U R C E L I S T I N G

## L I N E S T M T

## I D F I E L D

192 > administrator obtain all sets of inc-audit-information  
 193 > for a particular subject with subject-id and object  
 194 > with object-id.

195 > PART OP: audsys;  
 196 > USES: sub-obj-audit-request;  
 197 > DERIVES: sub-obj-audit-trail;

198 >  
 199 > PROCESS: sub-inc-audit;  
 200 > SYNONYM: subincand;  
 201 > DESCRIPTION;

202 > This process allows the system security  
 203 > administrator obtain all sets of obj-audit-information  
 204 > for a particular subject with subject-id and incident  
 205 > with incident-type.

206 > PART OP: audsys;  
 207 > USES: sub-inc-audit-request;  
 208 > DERIVES: sub-inc-audit-trail;

209 >  
 210 > PROCESS: sub-obj-inc-audit;  
 211 > SYNONYM: subobjincand;  
 212 > DESCRIPTION;

213 > This process allows the system security  
 214 > administrator obtain all sets of audit-information  
 215 > for a particular subject with subject-id, object with  
 216 > object-id, and incident with incident-type.

217 > PART OP: audsys;  
 218 > USES: sub-obj-inc-audit-request;  
 219 > DERIVES: sub-obj-inc-audit-trail;

220 >  
 221 > PROCESS: sub-audit;  
 222 > SYNONYM: subaud;  
 223 > DESCRIPTION;

224 > This process allows the system security  
 225 > administrator obtain all sets of obj-inc-audit-  
 226 > information for a particular subject with subject-id.

227 > PART OP: audsys;  
 228 > USES: sub-audit-request;  
 229 > DERIVES: sub-audit-trail;

230 >

## A S - I S S O U R C E L I S T I N G

LINE S Y M T

ID FIELD

```

231 > PROCESS:   obj-inc-audit;
232 > SYNONYM:   obj-inc-audit;
233 > DESCRIPTION:
234 >
235 > This process allows the system security
236 > administrator obtain all sets of sub-audit-information
237 > for a particular object with object-id and incident
238 > with incident-id.
239 > PART OF:   audsys;
240 > USES:      obj-inc-audit-request;
241 > DERIVES:   obj-inc-audit-trail;
242 >
243 > PROCESS:   obj-audit;
244 > SYNONYM:   obj-audit;
245 > DESCRIPTION:
246 >
247 > This process allows the system security
248 > administrator obtain all sets of sub-inc-audit-
249 > information for a particular object with object-id.
250 > PART OF:   audsys;
251 > USES:      obj-audit-request;
252 > DERIVES:   obj-audit-trail;
253 >
254 > PROCESS:   inc-audit;
255 > SYNONYM:   inc-audit;
256 > DESCRIPTION:
257 >
258 > This process allows the system security
259 > administrator obtain all sets of sub-obj-audit-
260 > information for a particular incident with incident-
261 > type.
262 > PART OF:   audsys;
263 > USES:      inc-audit-request;
264 > DERIVES:   inc-audit-trail;
265 >
266 > PROCESS:   dump-audit;
267 > SYNONYM:   dump-audit;
268 > DESCRIPTION:
269 >
270 > This process allows the system security
271 > administrator obtain all sets of sub-obj-audit-
272 > information available in the auditing-system-data-

```

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```

270 > base. ;
271 > PART OP: audsys;
272 > USES: dump-audit-request;
273 > DERIVES: dump-audit-trail;
274 >
275 > /* Reference Monitor Subfunctions */
276 > /* The following statements demonstrate how low level */
277 > /* functions may be defined. */
278 >
279 > PROCESS: check-need-to-know-usage;
280 > DESCRIPTION:
281 > This process checks if a subject-need-to-know-
282 > object relation with usage-attribute exists
283 > between subject with subject-id and object with
284 > object-id. ;
285 > KEYWORD: low-level;
286 > USES: subject-id,object-id,usage-attribute TO
287 > DERIVE: error-code;
288 >
289 > PROCESS: check-sub-obj-sec-levels;
290 > DESCRIPTION:
291 > This process checks if sub-curr-sec-level
292 > exceeds obj-sec-level. For example, security level 1
293 > exceeds security level 2 if the classification level
294 > of security level 1 is higher than the classification
295 > level of security level 2 and the category set of
296 > security level 2 is a subset of the category set of
297 > security level 1. ;
298 > KEYWORD: low-level;
299 > USES: sub-curr-sec-level,obj-sec-level TO
300 > DERIVE: error-code;
301 >
302 > PROCESS: create-access-relation;
303 > DESCRIPTION:
304 > This process creates a subject-access-to-object
305 > relation between subject with subject-id and object with
306 > object-id. ;
307 > KEYWORD: low-level;
308 > USES: subject-id,object-id TO

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```

309 > UPDATE:      usage-attribute;
310 > MAINTAINS:    subject-access-to-object;
311 >
312 > PROCESS:      produce-audit-incident;
313 > DESCRIPTION:
314 > This process produces an occurrence of incident-
315 > information in the auditing system data base based on
316 > the value of error-code. ;
317 > KEYWORD:      low-level;
318 > USES:          error-code TO
319 > DERIVE:        incident-information;
320 >
321 > PROCESS:      generate-decision;
322 > DESCRIPTION:
323 > This process derives a decision type based on
324 > the value of error-code. ;
325 > KEYWORD:      low-level;
326 > USES:          error-code TO
327 > DERIVE:        decision-type;
328 >
329 > PROCESS:      check-access-usage;
330 > DESCRIPTION:
331 > This process checks if a subject-access-to-
332 > object relation with usage attribute exist between
333 > subject with subject-id and object with object-id. ;
334 > KEYWORD:      low-level;
335 > USES:          subject-id,object-id,usage-attribute TO
336 > DERIVE:        error-code;
337 >
338 > PROCESS:      delete-access-relation;
339 > DESCRIPTION:
340 > This process deletes a subject-access-to-object
341 > relation with usage attribute between subject with
342 > subject-id and object with object-id. ;
343 > KEYWORD:      low-level;
344 > USES:          subject-id,object-id TO
345 > DERIVE:        error-code;
346 >
347 > PROCESS:      create-object-information;

```

## A S - I S   S O U R C E   L I S T I N G

ID FIELD

LINE S T M T

```

348 > DESCRIPTION;
349 > This process creates an occurrence of object-
350 > information in the appropriate set according to the value
351 > of obj-sec-level and sets the value of object-location.;
352 > KEYWORD: low-level;
353 > USES: object-id,obj-sec-level TO
354 > DERIVE: object-information;
355 >
356 > PROCESS: delete-object-information;
357 > DESCRIPTION;
358 > This process deletes an occurrence of object-
359 > information from the appropriate set based on the values
360 > of object-id and obj-sec-level. ;
361 > KEYWORD: low-level;
362 > USES: object-id,obj-sec-level TO
363 > DERIVE: error-code;
364 >
365 > /* procedures for Reference Monitor Functions */
366 >
367 > PROCESS: get-read;
368 > UTILIZES: check-need-to-know-usage,
369 > check-sub-obj-sec-levels,
370 > create-access-relation,
371 > produce-audit-incident,
372 > generate-decision;
373 >
374 > PROCEDURE:
375 > 1. Check if subject-need-to-know-object relation exists
376 > with usage-attribute value of read between subject with
377 > subject-id and object with object-id. If answer is
378 > no, go to step 4.
379 > 2. Otherwise, check if subject's sub-curr-sec-level
380 > exceeds object's obj-sec-level. If answer is no,
381 > go to step 4.
382 > 3. Otherwise, create a subject-access-to-object relation
383 > with usage-attribute between subject with subject-id
384 > and object with object-id.
385 > 4. produce an audit incident and generate a decision
386 > based on the value of error-code and then terminate. ;

```

## A S - I S S O U R C E L I S T I N G

ID FIELD

LINE S T M T

```

387 > PROCESS:  release-usage-attr;
388 > UTILIZES:  check-access-usage,
389 >             delete-access-relation,
390 >             produce-audit-incident,
391 >             generate-decision;
392 >
393 > PROCEDURE:
394 > 1. Check if subject-access-to-object relation exists
395 >    with usage-attribute between subject with subject-id
396 >    and object with object-id. If answer is no, go to
397 >    step 3.
398 > 2. Otherwise, delete the relation.
399 > 3. Produce an audit incident and generate a decision based
400 >    on the value of error-code and then terminate. ;
401 >
402 > PROCESS:  create-object;
403 > UTILIZES:  check-sub-obj-sec-levels,
404 >             create-object-information,
405 >             produce-audit-incident,
406 >             generate-decision;
407 >
408 > PROCEDURE:
409 > 1. Check if subject's sub-curr-sec-level exceeds object's
410 >    obj-sec-level. If answer is no, go to step 3.
411 > 2. Create an occurrence of object-information with
412 >    object-id in the appropriate file based on the value
413 >    of obj-sec-level.
414 > 3. Produce an audit incident and generate a decision
415 >    based on the value of error-code and then terminate. ;
416 >
417 > RELATION:  subject-access-to-object;
418 > DERIVATION:
419 > Create-access-relation adds connections and
420 > delete-access-relation deletes connections. ;
421 > MAINTAINED BY: delete-access-relation;
422 >
423 > SET:      topsecfile,secfile,confile,uncfile;
424 > DERIVATION:
425 > Create-object-information adds objects to these sets
426 > and delete-object-information deletes objects from

```

A S - I S S O U R C E L I S T I N G

LINE S T M T

426 >  
427 >  
428 > EOP

these sets. :

ID FIELD

## Security-control-example

## DATA BASE SUMMARY

ATTRIBUTE	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE-VALUE	2	1	50.00	1	50.00
ELEMENT	4	0		0	
ENTITY	15	0		12	80.00
GROUP	3	3	100.00	3	100.00
INPUT	11	8	72.73	3	27.27
KEYWORD	27	27	100.00	4	14.81
MEMO	3	0		2	66.67
OUTPUT	1	0		1	100.00
PROCESS	27	27	100.00	4	14.81
INTERFACE	36	27	75.00	36	100.00
RELATION	3	3	100.00	3	100.00
SET	5	0		5	100.00
	7	7	100.00	7	100.00
** TOTAL **	144	103	71.53	31	56.25

## Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ELE' ORDER=BYTYPE

1	category-set	ELEMENT
2	classification-level	ELEMENT
3	consol-nr	ELEMENT
4	date-time	ELEMENT
5	decision-type	ELEMENT
6	error-code	ELEMENT
7	incident-type	ELEMENT
8	object-id	ELEMENT
9	object-location	ELEMENT
10	receiving-subject-id	ELEMENT
11	requesting-subject-id	ELEMENT
12	security-id	ELEMENT
13	subject-id	ELEMENT
14	usage-attribute	ELEMENT
15	validation-code	ELEMENT



DATA PROCESS REPORT

DATA PROCESS INTERACTION MATRIX

(i, j) value meaning

R Row i is received or used by column j (input)  
 U Row i is updated by column j  
 D Row i is derived or generated by column j (output)  
 A Row i is input to, updated by, and output of column j (all)  
 F Row i is input to and output of column j (flow)  
 1 Row i is input to and updated by column j  
 2 Row i is updated by and output of column j

	1	2	3	4	5	6	7	8	9
1	I								
2	I	I							
3	I	I	I						
4	I	I	I	I					
5	I	I	I	I	I				
6	I	R	D	D	D	I	D	R	I
7	I	I							
8	I	R	R	I	R	R	R	I	I
9	I	I							
10	I	I							
11	I								
12	I	I							
13	I	R	R	R	I				R
14	I	R	R	R	I				I
15	I								

## DATA PROCESS REPORT

## DATA PROCESS INTERACTION MATRIX ANALYSIS

## DATA

----

category-set	(ELEMENT)	(ROW	1)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
classification-level	(ELEMENT)	(ROW	2)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
console-nr	(ELEMENT)	(ROW	3)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
date-time	(ELEMENT)	(ROW	4)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
incident-type	(ELEMENT)	(ROW	7)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
object-location	(ELEMENT)	(ROW	9)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
receiving-subject-id	(ELEMENT)	(ROW	10)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
requesting-subject-id	(ELEMENT)	(ROW	11)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
security-id	(ELEMENT)	(ROW	12)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS
validation-code	(ELEMENT)	(ROW	15)	NOT DERIVED,	UPDATED,	OR USED BY	ANY PROCESS

## PROCESSES

-----

check-sub-obj-sec-levels  
 produce-audit-incident  
 create-object-information

(COLUMN 3) DERIVES SOMETHING, BUT DOES NOT USE ANYTHING  
 (COLUMN 7) USES DATA, BUT DOES NOT DERIVE OR UPDATE ANYTHING  
 (COLUMN 3) USES DATA, BUT DOES NOT DERIVE OR UPDATE ANYTHING

DATA PROCESS REPORT

PROCESS INTERACTION MATRIX (INCIDENCE)

The rows and columns are process names from above.  
 An asterisk in (i,j) means that something derived  
 or updated by process i is used by process j.

		123456789	
1	I		I
2	I*	*	I
3	I*	*	I
4	I*	*	I
5	I*	*	I
6	J*	*	I
7	I		I
8	I		I
9	I*	*	I

DATA PROCESS REPORT

PROCESS INTERACTION MATRIX ANALYSIS

generate-decision	(ROW/COL	1) NO SUCCESSORS FOR THIS PROCESS
check-sub-obj-sec-levels	(ROW/COL	3) NO PREDECESSORS FOR THIS PROCESS
delete-access-relation	(ROW/COL	5) NO PREDECESSORS FOR THIS PROCESS
delete-object-information	(ROW/COL	6) NO PREDECESSORS FOR THIS PROCESS
produce-audit-incident	(ROW/COL	7) NO SUCCESSORS FOR THIS PROCESS
create-object-information	(ROW/COL	8) NO INTERACTION WITH OTHER PROCESSES
create-access-relation	(ROW/COL	9) NO PREDECESSORS FOR THIS PROCESS

URA VERSION 3.0R1

Security-control-example

JUN 16, 1976 00:49:28

PAGE

91

EXTENDED PICTURE

PARAMETERS FOR: EP

NAME=create-access-relation DATA-FLOW NOSTRUCTURE FORWARD NOBACKWARD LINKS=1000 NOINDEX  
COLUMNS=119 ROWS=39 HORIZONTAL-BOXES=6 VERTICAL-BOXES=6

## Security-control-example

## EXTENDED PICTURE

```
--PROCESS--+
create-      I
access-      I ..... Iattribute I
relation     I
-----+
+--ELEMENT--+
usage-      I
Iattribute  I
+--UPDATED--+
+--PROCESS--+
create-      I
access-      I ..... Iattribute I
relation     I
-----+
+--PROCESS--+
Icheck-      I
Iaccess-     I ..... Ierror-code I
Iusage       I
+USES TO DRV+
+--ELEMENT--+
Ierror-code I
Ierror-code I
+--DERIVED--+
+--PROCESS--+
Icheck-need-I
Ito-         I ..... Ierror-code I
Iknow-usage  I
+USES TO DRV+
+--ELEMENT--+
Ierror-code I
Ierror-code I
+--DERIVED--+
+--PROCESS--+
Igenerate-   I
Idecision    I ..... Itype
I           I
+USES TO DRV+
+--ELEMENT--+
Ierror-code I
Ierror-code I
+--DERIVED--+
+--PROCESS--+
Iproduce-      I
Iaudit-      I ..... Iinforma
Iincident    I
+USES TO DRV+
+--ELEMENT--+
Ierror-code I
Ierror-code I
+--DERIVED--+
+--PROCESS--+
Iloops to    I
Iprevious    I ..... Ientry
Ientry       I
+--ELEMENT--+
Ierror-code I
Ierror-code I
+--DERIVED--+
```

## A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNJ

SOURCE NOXREF UPDATE DBREF

LINE S T M T

ID FIELD

```

1 > /* SCS system size */
2 >
3 > DEFINE: number-of-subjects SYSTEM-PARAMETER;
4 > DFSCRIPTION:
5 > This is the number of subjects for which
6 > information exists in the security control system. ;
7 > ATTRIBUTE: parameter-value varying;
8 >
9 > DEFINE: number-of-objects SYSTEM-PARAMETER;
10 > DESCRIPTION:
11 > This is the number of objects for which
12 > information exists in the security control system. ;
13 > ATTRIBUTE: parameter-value varying;
14 >
15 > DEFINE: number-of-incidents SYSTEM-PARAMETER;
16 > DFSCRIPTION:
17 > This is the number of incidents for which
18 > information exists in the security control system. ;
19 > ATTRIBUTE: parameter-value varying;
20 >
21 > DEFINE: number-of-levels SYSTEM-PARAMETER;
22 > DESCRIPTION:
23 > This is the number of different classification
24 > levels which may be specified as a part of a subject
25 > and object security level. ;
26 > ATTRIBUTE: parameter-value fixed;
27 > VALUE: 7;
28 >
29 > DEFINE: number-of-categories SYSTEM-PARAMETER;
30 > DFSCRIPTION:
31 > This is the number of categories which are
32 > available for inclusion in a category set which may
33 > be specified as a part of a subject and object security
34 > level. ;
35 > ATTRIBUTE: parameter-value fixed;

```

## A S - I S S O U R C E L I S T I N G

## LINE S T M T

## ID FIELD

```

36 > VALUE: 16;
37 >
38 > DEFINE: total-objects-and-subjects SYSTEM-PARAMETER:
39 > DESCRIPTION:
40 > This is the sum of number-of-objects and number-
41 > of-subjects.
42 > ATTRIBUTE: parameter-value varying;
43 >
44 > DEFINE: number-of-audit-audit SYSTEM-PARAMETER:
45 > ATTRIBUTE: parameter-value subject-to-change:
46 > VALUE IS: 1;
47 >
48 > DEFINE: number-of-obj-audit SYSTEM-PARAMETER:
49 > ATTRIBUTE: parameter-value subject-to-change:
50 > VALUE IS: 1;
51 >
52 > DEFINE: number-of-sub-audit SYSTEM-PARAMETER:
53 > ATTRIBUTE: parameter-value subject-to-change:
54 > VALUE IS: 1;
55 >
56 > ENTITY: subject-information;
57 > CARDINALITY: number-of-subjects;
58 >
59 > ENTITY: object-information;
60 > CARDINALITY: number-of-objects;
61 >
62 > ENTITY: incident-information;
63 > CARDINALITY: number-of-incidents;
64 >
65 > ELEMENT: consol-nr;
66 > VALUES ARE: 0 THRU 25;
67 >
68 > SPT: reference-monitor-data-base;
69 > CARDINALITY: total-objects-and-subjects;
70 >
71 > RELATION: subject-need-to-know-object;
72 > CONNECTIVITY: many TO many;
73 >
74 > RELATION: subject-access-to-object;

```

## A S - Y S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```
75 > CONNECTIVITY: many TO many;
76 >
77 > RELATION: sub-obj-audit-relation;
78 > CONNECTIVITY: many TO many;
79 >
80 > RELATION: sub-inc-audit-relation;
81 > CONNECTIVITY: 1 TO many;
82 > CARDINALITY: number-of-incidents;
83 >
84 > RELATION: obj-inc-audit-relation;
85 > CONNECTIVITY: 1 TO many;
86 >
87 > OUTPUT: dump-audit-trail;
88 > CONSISTS: number-of-incidents sub-obj-inc-audit-information;
89 >
90 > INTERVAL: year;
91 > CONSISTS: 12 month;
92 > CONSISTS: 52 week;
93 > CONSISTS: 365 day;
94 >
95 > INTERVAL: day; 24 hour;
96 > CONSISTS:
97 >
98 > INTERVAL: hour;
99 > CONSISTS: 60 minute;
100 >
101 > PROCESS: dump-audit;
102 > HAPPENS: number-of-dump-audit TIMES-PER month;
103 >
104 > INPUT: dump-audit-request;
105 > HAPPENS: number-of-dump-audit TIMES-PER month;
106 >
107 > OUTPUT: dump-audit-trail;
108 > HAPPENS: number-of-dump-audit TIMES-PER month;
109 >
110 > PROCESS: obj-audit;
111 > HAPPENS: number-of-obj-audit TIMES-PER month;
112 >
113 > INPUT: obj-audit-request;
```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```
114 > HAPPENS: number-of-obj-audit TIMES-PER month;
115 >
116 > OUTPUT: obj-audit-trail;
117 > HAPPENS: number-of-obj-audit TIMES-PER month;
118 >
119 > PROCESS: sub-audit;
120 > HAPPENS: number-of-sub-audit TIMES-PER month;
121 >
122 > INPUT: sub-audit-request;
123 > HAPPENS: number-of-sub-audit TIMES-PER month;
124 >
125 > OUTPUT: sub-audit-trail;
126 > HAPPENS: number-of-sub-audit TIMES-PER month;
127 >
128 > EOF
```

## Security-control-example

## DATA BASE SUMMARY

ATTRIBUTE	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE-VALUE	3	1	33.33	1	33.33
ELEMENT	7	0		0	
ENTITY	15	0		12	80.00
GROUP	3	3	100.00	3	100.00
INPUT	11	8	72.73	3	27.27
INTERVAL	27	27	100.00	4	14.81
KEYWORD	6	0		0	
MEMO	3	0		2	66.67
OUTPUT	1	0		1	100.00
PROCESS	27	27	100.00	4	14.81
INTERFACE	36	27	75.00	36	100.00
RELATION	2	3	100.00	3	100.00
SET	5	0		5	100.00
SYSTEM-PARAMETER	7	7	100.00	7	100.00
	10	0		6	60.00
** TOTAL **	164	103	62.80	87	53.05

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='SYSP' ORDER=BYTYPE

1	many	SYSTEM-PARAMETER
2	number-of-categories	SYSTEM-PARAMETER
3	number-of-dump-audit	SYSTEM-PARAMETER
4	number-of-incidents	SYSTEM-PARAMETER
5	number-of-levels	SYSTEM-PARAMETER
6	number-of-obj-audit	SYSTEM-PARAMETER
7	number-of-objects	SYSTEM-PARAMETER
8	number-of-sub-audit	SYSTEM-PARAMETER
9	number-of-subjects	SYSTEM-PARAMETER
10	total-objects-and-subjects	SYSTEM-PARAMETER

## Security-control-example

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

```

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMAPG=70 CMARG=1 HMARG=40 DESG
ONE-PER-LINE DEFINE COMMENT NONFW-PAGE NONFW-LINE

```

```

1 DEFINE
2   AS A SYSTEM-PARAMETER;
3   /* LEFT CONNECTIVITY OF:
4
5
6   /* RIGHT CONNECTIVITY OF:
7
8
9
10
11
12 DEFINE
13   AS A SYSTEM-PARAMETER;
14   DESCRIPTION:
15
16   This is the number of categories which are
17   available for inclusion in a category set which may
18   be specified as a part of a subject and object security
19   level.;
20   ATTRIBUTES ARE:
21     parameter-value
22     VALUE IS:
23
24   DEFINE
25     AS A SYSTEM-PARAMETER;
26     ATTRIBUTES ARE:
27       parameter-value
28       /* dump-audit HAPPENS
29       number-of-dump-audit TIMES-PER month /*
30       /* dump-audit-request HAPPENS
31       number-of-dump-audit TIMES-PER month /*
32       /* dump-audit-trail HAPPENS
33       number-of-dump-audit TIMES-PER month /*
34       VALUE IS:
35
36   DEFINE
37     AS A SYSTEM-PARAMETER;
38     number-of-incidents

```

many

```

subject-need-to-know-object,
subject-access-to-object,
sub-obj-audit-relation */
subject-need-to-know-object,
subject-access-to-object,
sub-obj-audit-relation,
sub-inc-audit-relation,
obj-inc-audit-relation */

```

number-of-categories

```

fixed;
16;

```

number-of-dump-audit

subject-to-change;

```

month /*
month /*
month /*
1;

```

number-of-incidents

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```
37 DESCRIPTION;
38
39      This is the number of incidents for which
40      information exists in the security control system.;
41      ATTRIBUTES ARE:
42      parameter-value
43      /* jump-audit-trail CONTAINS
44      number-of-incidents
45      */
46      /* CARDINALITY OF:
47
48      DEFINE
49      AS A SYSTEM-PARAMETER;
50      DESCRIPTION;
51
52      This is the number of different classification
53      levels which may be specified as a part of a subject
54      and object security level.;
55      ATTRIBUTES ARE:
56      parameter-value
57      VALUE IS:
58
59      fixed;
60      7;
61
62      number-of-obj-audit
63
64      subject-to-change;
65
66      month */
67
68      month */
69
70      month */
71      1;
72
73      number-of-objects
74
75      DEFINE
76      AS A SYSTEM-PARAMETER;
77      DESCRIPTION;
78
79      This is the number of objects for which
80      information exists in the security control system.;
81      ATTRIBUTES ARE:
82      parameter-value
83      /* CARDINALITY OF:
84
85      varying;
86      object-information */
```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

78 DEFINE
79   AS A SYSTEM-PARAMETER;
80   ATTRIBUTES ARE:
81     parameter-value
82   /* sub-audit HAPPENS
83     number-of-sub-audit TIMES-PER
84   /* sub-audit-request HAPPENS
85     number-of-sub-audit TIMES-PER
86   /* sub-audit-trail HAPPENS
87     number-of-sub-audit TIMES-PER
88   VALUE IS:
89     1;
90
91 DEFINE
92   AS A SYSTEM-PARAMETER;
93   DESCRIPTION;
94     This is the number of subjects for which
95     information exists in the security control system.;
96   ATTRIBUTES ARE:
97     parameter-value
98   /* CARDINALITY OF:
99     varying;
100     subject-information */
101     total-objects-and-subjects
102
103   AS A SYSTEM-PARAMETER;
104   DESCRIPTION;
105     This is the sum of number-of-objects and number-
106     of-subjects.;
107   ATTRIBUTES ARE:
108     parameter-value
109   /* CARDINALITY OF:
110     varying;
111     reference-monitor-data-base */
112   EOP EOP EOP EOP

```

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='INTERVAL' ORDER=BYTYPE

1	day	INTERVAL
2	hour	INTERVAL
3	minute	INTERVAL
4	month	INTERVAL
5	week	INTERVAL
6	year	INTERVAL

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: PDS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=70 CMARG=1 HMARG=40 DESG  
 ONE-PER-LINE DEFINE COMMENT NONPW-PAGE NONPW-LINE

1	INTERVAL	day;
2	CONSISTS OF:	
3	24	hour;
4	/* year CONSISTS OF 365	day */
5		
6	INTERVAL	hour;
7	CONSISTS OF:	
8	60	minute;
9	/* day CONSISTS OF 24	hour */
10		
11	INTERVAL	minute;
12	/* hour CONSISTS OF 60	minute */
13		
14	INTERVAL	month;
15	/* year CONSISTS OF 12	month */
16	/* dump-audit HAPPENS	
17	number-of-dump-audit TIMES-PER	month */
18	/* dump-audit-request HAPPENS	
19	number-of-dump-audit TIMES-PER	month */
20	/* dump-audit-trail HAPPENS	
21	number-of-dump-audit TIMES-PER	month */
22	/* obj-audit HAPPENS	
23	number-of-obj-audit TIMES-PER	month */
24	/* obj-audit-request HAPPENS	
25	number-of-obj-audit TIMES-PER	month */
26	/* obj-audit-trail HAPPENS	
27	number-of-obj-audit TIMES-PER	month */
28	/* sub-audit HAPPENS	
29	number-of-sub-audit TIMES-PER	month */
30	/* sub-audit-request HAPPENS	
31	number-of-sub-audit TIMES-PER	month */
32	/* sub-audit-trail HAPPENS	
33	number-of-sub-audit TIMES-PER	month */
34		
35	INTERVAL	week;
36	/* year CONSISTS OF 52	week */

URA VERSION 3.0P1

Security-control-example

JUN 16, 1976 20:40:28

PAGE

107

FORMATTED PROBLEM STATEMENT

37  
38 INTERVAL  
39 CONSISTS OF:  
40 12  
41 52  
42 365  
43  
44 EOF EOF EOF EOF EOF

year;  
month,  
week,  
day;

FREQUENCY REPORT

INTERVAL: month

NAME	TYPE	TIMES	HAPPEN S
dump-audit	PROCESS	number-of-dump-audit	
dump-audit-request	INPUT	number-of-dump-audit	
dump-audit-trail	OUTPUT	number-of-dump-audit	
obj-audit	PROCESS	number-of-obj-audit	
obj-audit-request	INPUT	number-of-obj-audit	
obj-audit-trail	OUTPUT	number-of-obj-audit	
sub-audit	PROCESS	number-of-sub-audit	
sub-audit-request	INPUT	number-of-sub-audit	
sub-audit-trail	OUTPUT	number-of-sub-audit	

## A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYN0

SOURCE NOXREF UPDATE DBREF

LINE S T M T

ID FIELD

```

1 > /* SCS system dynamics */
2 >
3 > ENTITY: subject-information;
4 > VOLATILITY:
5 > The sub-max-sec-level can only be changed by a
6 > system security administrator and only on decision
7 > of the administrator. The sub-curr-sec-level may
8 > change several times within the course of one session
9 > on the system. ;
10 >
11 > ENTITY: object-information;
12 > VOLATILITY:
13 > The obj-sec-level may be changed by either the
14 > owner of the object or the system security administrator.
15 > Changing the object-location is done based on need by
16 > the operating system. ;
17 >
18 > ENTITY: incident-information;
19 > VOLATILITY:
20 > The contents of this type of entity are never
21 > changed after creation. ;
22 >
23 > SET: reference-monitor-data-base;
24 > VOLATILITY-SET:
25 > The set is changed whenever a subject or object
26 > is added to, or deleted from, the system. ;
27 > VOLATILITY-NEWREP:
28 > Volatility of the set's members can be found
29 > under description for subject-information and object-
30 > information. ;
31 >
32 > SET: auditing-system-data-base;
33 > VOLATILITY-SET:
34 > The set is changed whenever an auditing incident
35 > occurs. ;

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```

36 > VOLATILITY-MEMBER:
37 >     An occurrence of incident-information is created
38 >     whenever an object is improperly accessed, a subject
39 >     logs in the system, or a subject id is improperly used. ;
40 >
41 > EVENT: occurrence-get-read-request;
42 >     TRIGGERS: get-read;
43 >     HAPPENS: get-read-listribution TIMES-PER hour;
44 >
45 > EVENT: initiate-get-read-procedure;
46 >     ON INCEPTION: get-read;
47 >     TRIGGERS: check-need-to-know-usage;
48 >
49 > PROCESS: check-need-to-know-usage;
50 >     TERMINATION-CAUSES: need-to-know-check-fails,
51 >                         need-to-know-check-succeeds;
52 >
53 > PROCESS: produce-audit-incident,generate-decision;
54 >     TRIGGERED BY: need-to-know-check-fails,
55 >                  sub-obj-sec-level-check-fails;
56 >
57 > PROCESS: check-sub-obj-sec-levels;
58 >     TRIGGERED BY: need-to-know-check-succeeds;
59 >     TERMINATION-CAUSES: sub-obj-sec-level-check-fails,
60 >                         sub-obj-sec-level-check-succ;
61 >
62 > PROCESS: create-access-relation;
63 >     TRIGGERED BY: sub-obj-sec-level-check-succ;
64 >
65 > EVENT: create-access-relation-succ;
66 >     ON TERMINATION: create-access-relation;
67 >     TRIGGERS: generate-decision;
68 >
69 > EVENT: need-to-know-check-fails;
70 >     WHEN need-to-know-check-passes BECOMES FALSE;
71 >
72 > EVENT: need-to-know-check-succeeds;
73 >     WHEN need-to-know-check-passes BECOMES TRUE;
74 >

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

```

75 > CONDITION: sub-obj-sec-level-check-passes;
76 > BECOMING TRUE IS CALLED sub-obj-sec-level-check-succ;
77 > BECOMING FALSE IS CALLED sub-obj-sec-level-check-fails;
78 >
79 > CONDITION: get-read-request-made;
80 > BECOMING TRUE CALLED occurrence-get-read-request;
81 > FALSE WHILE;
82 > Requests on the get-read procedure occur on
83 > demand of subjects. These occurrences are unscheduled
84 > and considered random events. ;
85 > TRUE WHILE;
86 > This event exists during the period in which the
87 > get-read-request is being processed up until the
88 > decision has been given to the subject. ;
89 >
90 > CONDITION: create-access-relation-fin;
91 > BECOMING TRUE CALLED create-access-relation-succ;
92 > FALSE WHILE;
93 > This event exists during the period in which
94 > the access relation is being created. This condition
95 > must resolve to a TRUE state unless there is an error
96 > in the software. ;
97 >
98 > EVENT: occur-release-usage-attr-req;
99 > TRIGGERS: release-usage-attr;
100 > HAPPENS: release-usage-attr-req-distr TIMES-per hour;
101 >
102 > EVENT: init-release-usage-attr-proc;
103 > ON INCEPTION release-usage-attr;
104 > TRIGGERS: check-access-usage;
105 >
106 > PROCESS: check-access-usage;
107 > TERMINATION-CAUSES: access-usage-check-fails,
108 > access-usage-check-succeeds;
109 >
110 > PROCESS: delete-access-relation;
111 > TRIGGERED BY: access-usage-check-succeeds;
112 >
113 > EVENT: delete-access-relation-succ;

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

TD FIELD

```

114 > ON TERMINATION: delete-access-relation;
115 > TRIGGERS: generate-decision;
116 >
117 > EVENT: access-usage-check-fails;
118 > TRIGGERS: produce-audit-incident,
119 > generate-decision;
120 >
121 > EVENT: occur-create-object-request;
122 > TRIGGERS: create-object;
123 > HAPPENS: create-object-distribution TIMES-PER hour;
124 >
125 > EVENT: init-create-object-procedure;
126 > ON INCEPTION: create-object;
127 > TRIGGERS: check-sub-obj-sec-levels;
128 >
129 > PROCESS: create-object-information;
130 > TRIGGERED BY: sub-obj-sec-level-check-succ;
131 >
132 > EVENT: create-object-information-succ;
133 > ON TERMINATION create-object-information;
134 > TRIGGERS: generate-decision;
135 >
136 > EOF

```

## Security-control-example

## DATA BASE SUMMARY

ATTRIBUTE	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE-VALUE	3	1	33.33	1	33.33
CONDITION	7	0		0	
ELEMENT	4	0		0	
ENTITY	15	0		12	80.00
EVENT	3	3	100.00	3	100.00
GROUP	15	0		0	
INPUT	11	8	72.73	3	27.27
INTERVAL	27	27	100.00	4	14.81
KEYWORD	6	0		0	
MEMO	3	0		2	66.67
OUTPUT	1	0		1	100.00
PROCESS	27	27	100.00	4	14.81
INTERPACE	36	27	75.00	36	100.00
RELATION	3	3	100.00	3	100.00
SPT	5	0		5	100.00
SYSTEM-PARAMETER	7	7	100.00	7	100.00
	13	0		6	46.15
** TOTAL **	186	103	55.38	87	46.77

URA VERSION 3.0R1

Security-control-example

JUN 16, 1976 00:49:28

PAGE

114

Process Chain

PARAMETERS FOR: PC

NAME=occur-release-usage-attr-req LINKS=1000 NOINDEX COLUMNS=119 ROWS=39 HORIZONTAL-BOXES=6  
VERTICAL-BOXES=6

## Process Chain

```

---EVENT---+
occur-rele-I
ase-usage--I .....
attr-req   I
-----+

+--PROCESS--+
Irelease-  I
Iusage-    I .....
Iattr      I
+--TRIGGERED--+

+---EVENT---+
Iinit-relea-I
Ise-usage-a-I .....
Itrr-proc   I
+ON INCEPTN+

+--PROCESS--+
Icheck-     I
Iaccess-    I .....
Iusage      I
+--TRIGGERED--+

+---EVENT---+
Iaccess-isa-I
Iqe-check-s-I .....
Iucceeds    I
+--ON TERM--+

+--PROCESS--+
Idelete-    I .....
Iaccess-    I .....
Irelatic    I .....
+--TRIGGE   I .....

+--PROCESS--+
Igenerat    I .....
Idecisio    I .....
I           I .....
+--TRIGGE   I .....

+--PROCESS--+
Iproduce      I .....
Iaudit-     I .....
Iincillen   I .....
+--TRIGGE   I .....

```

## Process Chain

```
+--PROCESS--+
Idelete- I
Iaccess- I ..... Idelete-acc-I
Irelation I ..... Iless-relati-r ..... I
+-TRIGGERED+-
+---EVENT+---+
Idelete-acc-I
Iless-relati-r I
Ion-succ I
+---ON TERM---+
+--PROCESS--+
Igenerate- I
Idecision I
I
+-TRIGGERED+-
```

```
+--PROCESS--+
Igenerate- I
Idecision I
I
+-TRIGGERED+-
```

```
+--PROCESS--+
Iproduce- I
Iaudit- I
Iincident I
+-TRIGGERED+-
```

```
+--PROCESS--+
Igenerate- I
Idecision I
I
+-TRIGGERED+-
```

## Security-control-example

## Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='EVENT' ORDER=BYTYPE

1	access-usage-check-fails	EVENT
2	access-usage-check-succeeds	EVENT
3	create-access-relation-succ	EVENT
4	create-object-information-succ	EVENT
5	delete-access-relation-succ	EVENT
6	init-create-object-procedure	EVENT
7	init-release-usage-attr-proc	EVENT
8	initiate-get-read-procedure	EVENT
9	need-to-know-check-fails	EVENT
10	need-to-know-check-succeeds	EVENT
11	occur-create-object-request	EVENT
12	occur-release-usage-attr-req	EVENT
13	occurrence-get-read-request	EVENT
14	sub-obj-sec-level-check-fails	EVENT
15	sub-obj-sec-level-check-succ	EVENT

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: PPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=70 CMARG=1 HMARG=40 DESG  
 ONE-PER-LINE DEFINE COMMENT NONFW-PAGE NONFW-LINE

1	EVENT		access-usage-check-fails;
2	TRIGGERS:		produce-audit-incident,
3			generate-decision;
4	ON TERMINATION OF:		check-access-usage;
5			
6	EVENT		access-usage-check-succeeds;
7	TRIGGERS:		delete-access-relation;
8	ON TERMINATION OF:		check-access-usage;
9			
10	EVENT		create-access-relation-succ;
11	TRIGGERS:		generate-decision;
12	WHEN:		create-access-relation-fin
13			BPCOMES TRUE;
14	ON TERMINATION OF:		create-access-relation;
15			
16	EVENT		create-object-information-succ;
17	TRIGGERS:		generate-decision;
18	ON TERMINATION OF:		create-object-information;
19			
20	EVENT		delete-access-relation-succ;
21	TRIGGERS:		generate-decision;
22	ON TERMINATION OF:		delete-access-relation;
23			
24	EVENT		init-create-object-procedure;
25	TRIGGERS:		check-sub-obj-sec-levels;
26	ON INCEPTION OF:		create-object;
27			
28	EVENT		init-release-usage-at-tr-proc;
29	TRIGGERS:		check-access-usage;
30	ON INCEPTION OF:		release-usage-attr;
31			
32	EVENT		initiate-get-read-procedure;
33	TRIGGERS:		check-need-to-know-usage;
34	ON INCEPTION OF:		get-read;
35			
36	EVENT		need-to-know-check-fails;

## FORMATTED PROBLEM STATEMENT

```

37 TRIGGERS:
38
39 WHEN:
40   produce-audit-incident,
41   generate-decision;
42   need-to-know-check-passes
43   BECOMES FALSE;
44   check-need-to-know-usage;
45
46 ON TERMINATION OF:
47   need-to-know-check-succeeds;
48   check-sub-obj-sec-levels;
49   need-to-know-check-passes
50   BECOMES TRUE;
51   check-need-to-know-usage;
52
53 ON TERMINATION OF:
54   occur-create-object-request;
55   create-object;
56
57 TRIGGERS:
58   hour;
59   occur-release-usage-attr-req;
60   release-usage-attr;
61
62 TRIGGERS:
63   hour;
64   occurrence-get-read-request;
65   get-read;
66   get-read-request-made
67   BECOMES TRUE;
68
69 TRIGGERS:
70   sub-obj-sec-level-check-fails;
71   produce-audit-incident,
72   generate-decision;
73   sub-obj-sec-level-check-passes
74   BECOMES FALSE;
75   check-sub-obj-sec-levels;
76
77 ON TERMINATION OF:
78   sub-obj-sec-level-check-succ;
79   create-access-relation,
80   create-object-information;

```

Security-control-example

FORMATTED PROBLEM STATEMENT

sub-obj-sec-level-check-passes;  
BECOMES TRUE;  
check-sub-obj-sec-levels;

78 WHEN:  
79  
80 ON TERMINATION OF:  
81  
82 EOF EOF EOF EOF EOF

URA VERSION 3.081

JUN 16, 1976 00:40:28

PAGE

121

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='COND' ORDER=RYTYPE

1	create-access-relation-fin	CONDITION
2	get-read-request-made	CONDITION
3	need-to-know-check-passes	CONDITION
4	sub-obj-sec-level-check-passes	CONDITION

FORMATTED PROBLEM STATEMENT

PARAMETERPS FOR: PPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=70 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINF COMMENT NONEN-PAGE NONEN-LINE

```

1 CONDITION
2 BECOMING TRUE IS CALLED:
3 FALSE WHILE;
4
5 This event exists during the period in which
6 the access relation is being created. This condition
7 must resolve to a TRUE state unless there is an error
8 in the software.;
9
10 CONDITION
11 BECOMING TRUE IS CALLED:
12 TRUE WHILE;
13
14 This event exists during the period in which the
15 get-read-request is being processed up until the
16 decision has been given to the subject.;
17
18 FALSE WHILE;
19
20 Requests on the get-read procedure occur on
21 demand of subjects. These occurrences are unscheduled
22 and considered random events.;
23
24 CONDITION
25 BECOMING TRUE IS CALLED:
26 BECOMING FALSE IS CALLED:
27
28 need-to-know-check-passes;
29 need-to-know-check-succeeds;
30 need-to-know-check-fails;
31
32 sub-obj-sec-level-check-passes;
33 sub-obj-sec-level-check-succ;
34 sub-obj-sec-level-check-fails;
35
36 EOF FOR FOR FOR FOR

```

## A S - I S S O U R C E L I S T I N G

## PARAMETERS FOR: SYN0

## SOURCE NOXPEP UPDATE DBREF

## LINE S T M T

## TD FIELD

```

1 > /* SCS project management */
2 >
3 > PROBLEM-DEFINER: michel-j-bastarache;
4 > MAILBOX: isdos-project-ann-arbor;
5 > RESPONSIBLE: auditing-system,
6 > administrative-security-system,
7 > reference-monitor,
8 > system-security-administrator;
9 >
10 > PROBLEM-DEFINER: james-m-amster;
11 > MAILBOX: isdos-project-ann-arbor;
12 > RESPONSIBLE: object-information,
13 > subject-information,
14 > incident-information,
15 > reference-monitor-subject;
16 >
17 > DEFINE: unclassified SECURITY;
18 > DESCRIPTION: Any parts of the problem statement
19 > designated as unclassified may be viewed
20 > by unclassified personnel. ;
21 > APPLIES: scs,scinp,scout,scint,scdb;
22 >
23 >
24 > DEFINE: scs-statement-of-need SOURCE;
25 > DFSCRIPTION: This document is the statement of need for the
26 > Security Control System.
27 > Distribution Data: 22 August 1975.
28 > It is directed towards the MACINS
29 > Multilevel Computer Security System. ;
30 > APPLIES: SCS;
31 >
32 >
33 > DEFINE: scs-specification SOURCE;
34 > DESCRIPTION: This document specifies the major functions of
35 >

```

## A S - I S S O U R C E L I S T I N G

LINE S T M T

ID FIELD

the security control system. The access controls or reference monitor, the auditing system, and the administrative security system are mentioned. ;

APPLIES: SCS:

MEMO: clearance-memo;

DESCRIPTION:

In this specification, clearance is defined as the eligibility of a person (or process or job) to access information of a certain classification level (or lower). For example, a person with a Secret clearance is eligible to access information with classification levels Unclassified to Secret, but may not have access to Top Secret information. When compartmented security is used, a clearance also includes the categories a person is eligible to access. In addition to the eligibility afforded a person by his clearance, he must also have the need to know the classified information before he is given access. ;

APPLIES: classification-level;

MEMO: category-set-memo;

DESCRIPTION:

In reference to a person (or process), a category set refers to the set of compartments a person is eligible to access. A compartment in this context is an orthogonal subdivision of the classification levels. A compartment is like a FORMAL NEED TO KNOW authorization to information of a certain topic without consideration of classification level.

In reference to documents, files, or other objects a category set refers to the possible information sources used to create the object. Thus, a category set with several categories or compartments would indicate that the object should be handled with extra caution or objects which would intersect the sensitive areas of each of the categories in the set. ;

APPLIES: category-set;

TRA VERSION 3.031

Security-control-example

JUN 16, 1976 00:42:28

PAGE 125

A S - I S   S O U R C E   L I S T I N G

LINE S T M T

75 > EOF

ID FIELD

## DATA BASE SUMMARY

ATTRIBUTE	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE-VALUE	3	1	33.33	1	33.33
CONDITION	7	0		0	
ELEMENT	4	0		0	
ENTITY	15	0		12	80.00
EVENT	3	3	100.00	3	100.00
GROUP	15	0		0	
INPUT	11	8	72.73	3	27.27
INTERVAL	27	27	100.00	4	14.81
KEYWORD	6	0		0	
MAILBOX	3	0		2	66.67
MEMO	1	0		0	
OUTPUT	3	0		3	100.00
PROBLEM-DEFINER	27	27	100.00	4	14.81
PROCFSS	2	0		0	
INTERFACE	36	27	75.00	36	100.00
RELATION	3	3	100.00	3	100.00
SECURITY	5	0		5	100.00
SET	1	0		1	100.00
SOURCE	7	7	100.00	7	100.00
SYSTEM-PARAMETER	2	0		2	100.00
	13	0		6	46.15
** TOTAL **	194	103	53.09	92	47.42

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='MAILBOX OR MEMO OR PD' ORDER=RYTYPE

- 1 isdos-project-ann-arbor
- 2 category-set-memo
- 3 clearance-memo
- 4 system-philosophy-memo
- 5 james-m-amster
- 6 michel-j-bastarache

MAILBOX  
MEMO  
MEMO  
MEMO  
PROBLEM-DEFINER  
PROBLEM-DEFINER

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 PMARG=70 CMARG=1 HMARG=40 DFSG  
 ONE-PER-LINE DEFINE COMMENT NONFW-PAGE NONFW-LINE

1 DEFINE  
 2 AS A MAILBOX;  
 3 APPLIES TO:  
 4  
 5 isdos-project-ann-arbor  
 6  
 7 michel-j-bastarache,  
 8 james-m-amster;

9  
 10 category-set-memo;  
 11  
 12  
 13  
 14  
 15  
 16  
 17  
 18  
 19  
 20  
 21  
 22  
 23  
 24  
 25  
 26  
 27  
 28  
 29  
 30  
 31  
 32  
 33  
 34  
 35  
 36

In reference to a person (or process), a category set refers to the set of compartments a person is eligible to access. A compartment in this context is an orthogonal subdivision of the classification levels. A compartment is like a FORMAL NEED TO KNOW authorization to information of a certain topic without consideration of classification level.

In reference to documents, files, or other objects a category set refers to the possible information sources used to create the object. Thus, a category set with several categories or compartments would indicate that the object should be handled with extra caution of objects which would intersect the sensitive areas of each of the categories in the set.;

category-set;

APPLIES TO:

clearance-memo;

DESCRIPTION;

In this specification, clearance is defined as the eligibility of a person (or process or job) to access information of a certain classification level (or lower). For example, a person with a Secret clearance is eligible to access information with classification levels unclassified to Secret, but may not have access to Top Secret information. When compartmented security is used, a clearance also includes the categories a person is eligible to access. In addition to the eligibility afforded a person by his clearance, he must also have the need to know the classified

## Security-control-example

## FORMATTED PROBLEM STATEMENT

37 information before he is given access.;  
38 classification-level;  
39  
40 MEMO  
41  
42 DESCRIPTION: The philosophy of the secure computer system will  
43 be such that the system will control the various shared  
44 resources. Hence the user will only be able to influence  
45 allocation decisions in a secondary way. Specifically,  
46 he can ask for a resource but not control the absolute  
47 time or address of the resource. It is essential that any  
48 other paths which might allow the user to access  
49 information (from any device) without the access controls  
50 of the system be eliminated.;

51 APPLIES TO:  
52 security-control-system,  
53 security-control-input,  
54 security-control-output,  
55 security-control-interface,  
56 security-control-data-base;

57 PROBLEM-DEFINER  
58 MAILBOX:  
59 RESPONSIBLE FOR:  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
james-m-amster;  
islos-project-ann-arbor;  
object-information,  
subject-information,  
incident-information,  
reference-monitor-subject;  
  
michel-j-bastarache;  
islos-project-ann-arbor;  
auditing-system,  
administrative-security-system,  
reference-monitor,  
system-security-administrator;

71 EOF EOF EOF EOF EOF

Name Generation

PARAMETERS FOR: NC

PRINT PUNCH EMPTY SELECTION='PD=james-m-amster' ORDER=BYTYPE

- 1 incident-information
- 2 object-information
- 3 subject-information
- 4 reference-monitor-subject

ENTITY  
ENTITY  
ENTITY  
INTERFACE

Security-control-example

DICTIONARY REPORT

PARAMETERS FOR: DICT

FILE NOINDEX DESCRIPTION SYNONYMS KEYWORDS RESPONSIBLE-PO NUM-SPACE=2

1 incident-information

ENTITY

DESCRIPTION:

This information holds data about where and when an incident has occurred.

SYNONYMS: incinfo

RESP PD: james-m-amster

2 object-information

ENTITY

DESCRIPTION:

This information holds identification, security, and location information for a particular object.

SYNONYMS: objinfo

RESP PD: james-m-amster

3 subject-information

ENTITY

DESCRIPTION:

This information holds identification and security data about a reference monitor subject.

SYNONYMS: subinfo

RESP PD: james-m-amster

4 reference-monitor-subject

INTERPACE

DICTIONARY REPORT

DESCRIPTION:

A reference monitor subject may be a user, a process, or a job which generates requests on the reference monitor.

SYNONYMS: rmonsub

KEYWORDS: level-2

RESP PD: james-m-amster

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='MEMO' ORDER=BYTYPE

- 1 category-set-memo
- 2 clearance-memo
- 3 svstem-philosophy-memo

MEMO  
MEMO  
MEMO

## PUNCHED COMMENT ENTRIES

## PARAMETERS FOR: PCOM

FILE DESCRIPTION NOPOCOPDURE NOVOLATILITY-MEMBER NOVOLATILITY-SET MODERIVATION  
NOTE- WHILE NOFALSE-WHILE PRINT PUNCH

1\* category-set-memo  
DESCRIPTION:

1 In reference to a person (or process), a category  
2 set refers to the set of compartments a person is  
3 eligible to access. A compartment in this context is  
4 an orthogonal subdivision of the classification  
5 levels. A compartment is like a FORMAL WHEN TO KNOW  
6 authorization to information of a certain topic  
7 without consideration of classification level.

8 In reference to documents, files, or other objects  
9 a category set refers to the possible information  
10 sources used to create the object. Thus, a category set  
11 with several categories or compartments would indicate  
12 that the object should be handled with extra caution  
13 of objects which would intersect the sensitive areas  
14 of each of the categories in the set.;

2\* clearance-memo  
DESCRIPTION:

1 In this specification, clearance is defined as the  
2 eligibility of a person (or process or job) to access  
3 information of a certain classification level (or  
4 lower). For example, a person with a Secret clearance  
5 is eligible to access information with classification  
6 levels Unclassified to Secret, but may not have access  
7 to Top Secret information. When compartmented security  
8 is used, a clearance also includes the categories a  
9 person is eligible to access. In addition to the  
10 eligibility afforded a person by his clearance, he  
11 must also have the need to know the classified  
12 information before he is given access.;

3\* system-philosophy-memo  
DESCRIPTION:

1 The philosophy of the secure computer system will

## PUNCHED COMMENT ENTRIES

2 be such that the system will control the various shared  
3 resources. Hence the user will only be able to influence  
4 allocation decisions in a secondary way. Specifically,  
5 he can ask for a resource but not control the absolute  
6 time or address of the resource. It is essential that any  
7 other paths which might allow the user to access  
8 information (from any device) without the access controls  
9 of the system be eliminated.;

NAME LIST

PARAMETERS FOR: NL

ORDER=BYTYPE

NAME	TYPE	SYNONYM
1 occurrences	ATTRIBUTE	
2 parameter-value	ATTRIBUTE	
3 specification-derivation	ATTRIBUTE	
4 explicit	ATTRIBUTE-VALUE	
5 fixed	ATTRIBUTE-VALUE	
6 implicit	ATTRIBUTE-VALUE	
7 scheduled	ATTRIBUTE-VALUE	
8 subject-to-change	ATTRIBUTE-VALUE	
9 unscheduled	ATTRIBUTE-VALUE	
10 varying	CONDITION	
11 create-access-relation-fin	CONDITION	
12 get-read-request-made	CONDITION	
13 need-to-know-check-passes	CONDITION	
14 sub-obj-sec-level-check-passes	CONDITION	
15 category-set	ELEMENT	
16 classification-level	ELEMENT	
17 consol-nr	ELEMENT	
18 date-time	ELEMENT	
19 decision-type	ELEMENT	
20 error-code	ELEMENT	
21 incident-type	ELEMENT	
22 object-id	ELEMENT	
23 object-location	ELEMENT	
24 receiving-subject-id	ELEMENT	
25 requesting-subject-id	ELEMENT	
26 security-id	ELEMENT	
27 subject-id	ELEMENT	
28 usage-attribute	ELEMENT	
29 validation-code	ELEMENT	
30 incident-information	ENTITY	incinfo
31 object-information	ENTITY	objinfo
32 subject-information	ENTITY	subinfo
33 access-usage-check-fails	EVENT	
34 access-usage-check-succeeds	EVENT	

## NAME LIST

NAME	TYPE	SYNONYM
35 create-access-relation-succ	EVENT	
36 create-object-information-succ	EVENT	
37 delete-access-relation-succ	EVENT	
38 init-create-object-procedure	EVENT	
39 init-release-usage-attr-proc	EVENT	
40 initiate-get-read-procedure	EVENT	
41 need-to-know-check-fails	EVENT	
42 need-to-know-check-succeeds	EVENT	
43 occur-create-object-request	EVENT	
44 occur-release-usage-attr-req	EVENT	
45 occurrence-get-read-request	EVENT	
46 sub-obj-sec-level-check-fails	EVENT	
47 sub-obj-sec-level-check-succ	EVENT	
48 audit-information	GROUP	audinfo
49 inc-audit-information	GROUP	incaudinfo
50 obj-audit-information	GROUP	objaudinfo
51 obj-inc-audit-information	GROUP	objincaudinfo
52 obj-sec-level	GROUP	
53 sub-audit-information	GROUP	subaudinfo
54 sub-curr-sec-level	GROUP	
55 sub-inc-audit-information	GROUP	subincaudinfo
56 sub-max-sec-level	GROUP	
57 sub-obj-audit-information	GROUP	subobjaudinfo
58 sub-obj-inc-audit-information	GROUP	subobjincaudinfo
59 administrative-security-comd	INPUT	adm scom
60 auditing-request	INPUT	aud req
61 change-obj-sec-level-request	INPUT	kf11 req
62 change-sub-curr-sec-level-req	INPUT	kf10 req
63 change-sub-max-sec-level-comd	INPUT	chsubmaxsecclevcom
64 create-object-request	INPUT	kf8 req
65 create-subject-command	INPUT	crsubcom
66 delete-object-request	INPUT	kf3 req
67 delete-subject-command	INPUT	delsubcom
68 dump-audit-request	INPUT	dum aud req
69 get-execute-request	INPUT	kf3 req
70 get-read-request	INPUT	kf1 req
71 get-read-write-request	INPUT	kf4 req
72 get-write-request	INPUT	kf2 req
73 give-usage-attr-request	INPUT	kf5 req

## NAME LIST

NAME	TYPE	SYNONYM
74 inc-audit-request	INPUT	incandreq
75 link-reference-monitor-command	INPUT	linkmoncom
76 obj-audit-request	INPUT	objaudreq
77 obj-inc-audit-request	INPUT	objincandreq
78 reference-monitor-request	INPUT	rmnreq
79 release-usage-atrr-request	INPUT	kf5req
80 rescind-usage-atrr-request	INPUT	kf7req
81 security-control-input	INPUT	scinp
82 sub-audit-request	INPUT	subaudreq
83 sub-inc-audit-request	INPUT	subincandreq
84 sub-obj-audit-request	INPUT	subobjaudreq
85 sub-obj-inc-audit-request	INPUT	subobjincandreq
86 reference-monitor-subject	INTERFACE	rmnsub
87 security-control-interface	INTERFACE	scint
89 system-security-administrator	INTERFACE	ssa
		ssadm
89 day	INTERVAL	-
90 hour	INTERVAL	-
91 minute	INTERVAL	-
92 month	INTERVAL	-
93 week	INTERVAL	-
94 year	INTERVAL	-
95 level-1	INTERVAL	-
96 level-2	INTERVAL	-
97 low-level	INTERVAL	-
98 islos-project-ann-anchor	KEYWORD	-
99 category-set-memo	KEYWORD	-
100 clearance-memo	KEYWORD	-
101 system-philosophy-memo	KEYWORD	-
102 administrative-security-resp	KEYWORD	-
103 audit-trail	KEYWORD	-
104 change-obj-sec-level-decision	KEYWORD	-
105 change-sub-curr-sec-level-dec	KEYWORD	-
106 change-sub-max-sec-level-resp	KEYWORD	-
107 create-object-decision	KEYWORD	-
108 create-subject-response	KEYWORD	-
109 delete-object-decision	KEYWORD	-
110 delete-subject-response	KEYWORD	-
111 dump-audit-trail	KEYWORD	-
		admsres
		audtra
		kf11dec
		kf10dec
		chasubmaxseclevres
		kf8dec
		cresubres
		kf9dec
		delsubres
		dumaudtra

## NAME LIST

NAME	TYPE	SYNONYM
112 get-execute-decision	OUTPUT	
113 get-read-decision	OUTPUT	kf3dec
114 get-read-write-decision	OUTPUT	kf1dec
115 get-write-decision	OUTPUT	kf4dec
116 give-usage-attr-decision	OUTPUT	kf2dec
117 inc-audit-trail	OUTPUT	kf5dec
118 link-reference-monitor-resp	OUTPUT	incandtra
119 obj-audit-trail	OUTPUT	linrmontes
120 obj-inc-audit-trail	OUTPUT	objaudtra
121 reference-monitor-decision	OUTPUT	objincandtra
122 release-usage-attr-decision	OUTPUT	rmonddec
123 rescind-usage-attr-decision	OUTPUT	kf5dec
124 security-control-outout	OUTPUT	kf7dec
125 sub-audit-trail	OUTPUT	scout
126 sub-inc-audit-trail	OUTPUT	subaudtra
127 sub-obj-audit-trail	OUTPUT	subincandtra
128 sub-obj-inc-audit-trail	OUTPUT	subobjaudtra
129 james-m-amster	OUTPUT	subobjincandtra
130 michel-j-bastarache	PROBLEM-DEFINER	
131 administrative-security-system	PROBLEM-DEFINER	
132 auditing-system	PROCESS	adassys
133 change-obj-sec-level	PROCESS	aulsvs
134 change-sub-curr-sec-level	PROCESS	kf11
135 change-sub-max-sec-level	PROCESS	kf10
136 check-access-usage	PROCESS	chasubmaxseclev
137 check-need-to-know-usage	PROCESS	
138 check-sub-obj-sec-levels	PROCESS	
139 create-access-relation	PROCESS	
140 create-object	PROCESS	kf3
141 create-object-information	PROCESS	
142 create-subject	PROCESS	cresub
143 delete-access-relation	PROCESS	
144 delete-object	PROCESS	kf3
145 delete-object-information	PROCESS	
146 delete-subject	PROCESS	delsub
147 dump-audit	PROCESS	dumaud
148 generate-decision	PROCESS	
149 get-execute	PROCESS	kf3
150 get-read	PROCESS	kf1

## NAME LIST

NAME	TYPE	SYNONYM
151 get-read-write	PROCESS	
152 get-write	PROCESS	kf4
153 give-usage-attr	PROCESS	kf2
154 inc-audit	PROCESS	kf6
155 link-reference-monitor	PROCESS	incaud
156 obj-audit	PROCESS	linrmon
157 obj-inc-audit	PROCESS	objaud
158 produce-audit-incident	PROCESS	oblincaud
159 reference-monitor	PROCESS	
160 release-usage-attr	PROCESS	access-control-system
161 rescind-usage-attr	PROCESS	rmon
162 security-control-system	PROCESS	kf5
		kf7
		scs
		scsvs
163 sub-audit	PROCESS	subaut
164 sub-inc-audit	PROCESS	subincaud
165 sub-obj-audit	PROCESS	subobjaud
166 sub-obj-inc-audit	PROCESS	subobjincaud
167 obj-inc-audit-relation	RELATION	
168 sub-inc-audit-relation	RELATION	
169 sub-obj-audit-relation	RELATION	
170 subject-access-to-object	RELATION	
171 subject-need-to-know-object	RELATION	
172 unclassified	SECURITY	
173 auditing-system-data-base	SET	autsvsdb
174 confidential-file	SET	confile
175 reference-monitor-data-base	SET	rmondb
176 secret-file	SET	secfile
177 security-control-data-base	SET	scdb
178 top-secret-file	SET	topsecfile
179 unclassified-file	SET	uncfile
180 scs-specification	SOURCE	
181 scs-statement-of-need	SOURCE	
182 create-object-distribution	SYSTEM-PARAMETER	
183 get-read-distribution	SYSTEM-PARAMETER	
184 many	SYSTEM-PARAMETER	
185 number-of-categories	SYSTEM-PARAMETER	
186 number-of-dump-audit	SYSTEM-PARAMETER	
187 number-of-incidents	SYSTEM-PARAMETER	

	NAME	NAME LIST	TYPE	SYNONYM
188	number-of-levels		SYSTEM-PARAMETER	-
189	number-of-obj-audit		SYSTEM-PARAMETER	-
190	number-of-objects		SYSTEM-PARAMETER	-
191	number-of-sub-audit		SYSTEM-PARAMETER	-
192	number-of-subjects		SYSTEM-PARAMETER	-
193	release-usage-attr-req-dist		SYSTEM-PARAMETER	-
194	total-objects-and-subjects		SYSTEM-PARAMETER	-

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ATTR' ORDER=BYTYPE

- 1 occurrences
- 2 parameter-value
- 3 specification-derivation

ATTRIBUTE  
ATTRIBUTE  
ATTRIBUTE

## Security-control-example

## ATTRIBUTE REPORT

## PARAMETERS FOR: PAV

## FILE

## 1\* ATTRIBUTE: occurrences

## APPLIES TO:

- 1 reference-monitor-request
- 2 administrative-security-command
- 3 auditing-request

## VALUE:

unscheduled  
unscheduled  
scheduled

## 2\* ATTRIBUTE: parameter-value

## APPLIES TO:

- 1 number-of-subjects
- 2 number-of-objects
- 3 number-of-incidents
- 4 number-of-levels
- 5 number-of-categories
- 6 total-objects-and-subjects
- 7 number-of-dump-audit
- 8 number-of-object-audit
- 9 number-of-sub-audit

## VALUE:

varying  
varying  
varying  
fixed  
fixed  
varying  
subject-to-change  
subject-to-change  
subject-to-change

## 3\* ATTRIBUTE: specification-derivation

## APPLIES TO:

- 1 security-control-system
- 2 security-control-input
- 3 security-control-output
- 4 security-control-interface
- 5 security-control-data-base

## VALUE:

explicit  
implicit  
implicit  
explicit  
implicit

Security-Control-example

PROCESS STRUCTURE

PARAMETERS FOR: STR

PROCESS INDENT=3 NOINDEX

COUNT LEVEL NAME

1	1	check-access-usage
2	1	check-need-to-know-usage
3	1	check-subj-sec-levels
4	1	create-access-relation
5	1	create-object-information
6	1	delete-access-relation
7	1	delete-object-information
8	1	generate-decision
9	1	produce-audit-incident
10	1	security-control-system
11	2	reference-monitor
12	3	get-read
13	3	get-write
14	3	get-execute
15	3	get-read-write
16	3	release-usage-attr
17	3	give-usage-attr
18	3	rescind-usage-attr
19	3	create-object
20	3	delete-object
21	3	change-subj-sec-level
22	3	change-subj-sec-level
23	2	administrative-security-system
24	3	create-subject
25	3	delete-subject

PROCESS STRUCTURE

COUNT	LEVEL	NAME
26	3	change-sub-max-sec-level
27	3	link-reference-monitor
28	2	auditing-system
29	3	sub-obj-audit
30	3	sub-inc-audit
31	3	sub-obj-inc-audit
32	3	sub-audit
33	3	obj-inc-audit
34	3	obj-audit
35	3	inc-audit
36	3	dump-audit

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	12	2	3	3	23

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='PROC' ORDER=BYTYPE

1	administrative-security-system	PROCESS
2	auditing-system	PROCESS
3	change-obj-sec-level	PROCESS
4	change-sub-curr-sec-level	PROCESS
5	change-sub-max-sec-level	PROCESS
6	check-access-usage	PROCESS
7	check-need-to-know-usage	PROCESS
8	check-sub-obj-sec-levels	PROCESS
9	create-access-relation	PROCESS
10	create-object	PROCESS
11	create-object-information	PROCESS
12	create-subject	PROCESS
13	delete-access-relation	PROCESS
14	delete-object	PROCESS
15	delete-object-information	PROCESS
16	delete-subject	PROCESS
17	dump-audit	PROCESS
18	generate-decision	PROCESS
19	get-execute	PROCESS
20	get-read	PROCESS
21	get-read-write	PROCESS
22	get-write	PROCESS
23	give-usage-attr	PROCESS
24	inc-audit	PROCESS
25	link-reference-monitor	PROCESS
26	obj-audit	PROCESS
27	obj-inc-audit	PROCESS
28	produce-audit-incident	PROCESS
29	reference-monitor	PROCESS
30	release-usage-attr	PROCESS
31	rescind-usage-attr	PROCESS
32	security-control-system	PROCESS
33	sub-audit	PROCESS
34	sub-inc-audit	PROCESS
35	sub-obj-audit	PROCESS
36	sub-obj-inc-audit	PROCESS

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE VOINDEX PRINT NOPUNCH SMARG=5 NMAPG=39 AMARG=7 BIAR3=39 RMAPG=70 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONEX-PAGE NONEX-LINE

1 PROCESS administrative-security-system;

2 SYNONYMS ARE: admsvs;

3 DESCRIPTION:

4 The system will define the administrative  
5 functions of the system security administrator, and will  
6 support his responsibility for maintaining control of  
7 users id's, passwords, and user classification level and  
8 category set.;

9 KEYWORDS:

10 PART OF:

11 SURPARTS ARE:

level-2;

security-control-system;

create-subject,

delete-subject,

change-sub-max-sec-level,

link-reference-monitor;

administrative-security-comd;

administrative-security-resp;

administrative-security-resp;

reference-monitor-data-base;

administrative-security-comd;

20 RESPONSIBLE-PROBLEM-DEFINER IS: michel-j-bastarache;

22 PROCESS

auditing-system;

audsys;

23 SYNONYMS ARE:

24 DESCRIPTION:

25 The system will provide an automatic capability to  
26 collect and record data regarding security related  
27 actions.;

28 KEYWORDS:

29 PART OF:

30 SURPARTS ARE:

level-2;

security-control-system;

sub-obj-audit,

sub-inc-audit,

sub-obj-inc-audit,

sub-audit,

obj-inc-audit,

obj-audit,

inc-audit,

36

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

37 RECEIVES:
38 GENERATES:
39 DERIVES:
40 USES:
41
42 RESPONSIBLE-PROBLEM-DEFINER IS:
43
44 dump-audit;
45 auditing-request;
46 audit-trail;
47 audit-trail;
48 auditing-request,
49 auditing-svsystem-data-base;
50 michel-j-bastarache;
51
52 change-obj-sec-level;
53 kf11;
54
55 This process decides whether or not subject with
56 subject-id may revise the security level of object
57 with object-id to the value of obj-sec-level.;
58
59 PART OF:
60 DERIVES:
61 USES:
62
63 reference-monitor;
64 change-obj-sec-level-decision;
65 change-obj-sec-level-request;
66
67 change-sub-curr-sec-level;
68 kf10;
69
70 This process decides whether or not subject with
71 subject-id may change his current security level to
72 sub-curr-sec-level.;
73
74 PART OF:
75 DERIVES:
76 USES:
77
78 reference-monitor;
79 change-sub-curr-sec-level-dec;
80 change-sub-curr-sec-level-reg;
81
82 change-sub-max-sec-level;
83 chasubmaxseclev;
84
85 This process allows the system security
86 administrator with security-id to change the maximum
87 security level of subject with subject-id to
88 sub-max-sec-level.;
89
90 PART OF:
91 DERIVES:
92 USES:
93
94 administrative-security-svsystem;
95 change-sub-max-sec-level-tesp;
96 change-sub-max-sec-level-commd;
97
98 check-access-usage;
99

```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

78      This process checks if a subject-access-to-
79      object relation with usage attribute exist between
80      subject with subject-id and object with object-id.;
81      low-level;
82      release-usage-attr;
83      error-code
84      subject-id,
85      object-id,
86      usage-attribute;
87      access-usage-check-fails,
88      access-usage-check-succeeds;
89      init-release-usage-attr-proc;
90
91  PROCESS
92  DESCRIPTION:
93      This process checks if a subject-need-to-know-
94      object relation with usage-attribute exists
95      between subject with subject-id and object with
96      object-id.;
97  KEYWORDS:
98  UTILIZED BY:
99  DERIVES:
100  USING:
101
102  TERMINATION-CAUSES:
103
104  TRIGGERED BY:
105
106  PROCESS
107  DESCRIPTION:
108      This process checks if sub-curr-sec-level
109      exceeds obj-sec-level. For example, security level 1
110      exceeds security level 2 if the classification level
111      of security level 1 is higher than the classification
112      level of security level 2 and the category set of
113      security level 2 is a subset of the category set of
114      security level 1.;
115  KEYWORDS:
116  UTILIZED BY:
117
118

```

low-level;  
release-usage-attr;  
error-code  
subject-id,  
object-id,  
usage-attribute;  
access-usage-check-fails,  
access-usage-check-succeeds;  
init-release-usage-attr-proc;

check-need-to-know-usage;

low-level;  
get-read;  
error-code  
subject-id,  
object-id,  
usage-attribute;  
need-to-know-check-fails,  
need-to-know-check-succeeds;  
initiate-get-read-procedure;

check-sub-obj-sec-levels;

low-level;  
get-read,  
create-object;

## FORMATTED PROBLEM STATEMENT

```

110 DERIVES:
120 USING:
121
122 TERMINATION-CAUSES:
123
124 TRIGGERED BY:
125
126
127 PROCESS
128 DESCRIPTION:
129     This process creates a subject-access-to-object
130     relation between subject with subject-id and object with
131     object-id.;
132
133 KEYWORDS:
134 UTILIZED BY:
135 MAINTAINS:
136 UPDATES:
137 USING:
138
139 TERMINATION-CAUSES:
140 TRIGGERED BY:
141
142 PROCESS
143     SYNONYMS ARE:
144     DESCRIPTION:
145     This process decides whether or not subject with
146     subject-id may add an object to the directory
147     hierarchy directly below directory object with
148     object-id. This added object is requested to have
149     security level obj-sec-level.;
150
151 PART OF:
152 UTILIZES:
153
154 DERIVES:
155 USPS:
156 PROCEDURE:
157     1. Check if subject's sub-curr-sec-level exceeds object's
158     obj-sec-level. If answer is no, go to step 3.
159     2. Create an occurrence of object-information with

```

error-code  
sub-curr-sec-level,  
obj-sec-level;  
sub-obj-sec-level-check-fails,  
sub-obj-sec-level-check-succ;  
need-to-know-check-succeeds,  
init-create-object-procedure;  
  
create-access-relation;  
  
low-level;  
get-read;  
subject-access-to-object;  
usage-attribute  
subject-id,  
object-id;  
create-access-relation-succ;  
sub-obj-sec-level-check-succ;  
  
create-object;  
kfr;

reference-monitor;  
check-sub-obj-sec-levels,  
create-object-information,  
produce-audit-incident,  
generate-decision;  
create-object-decision;  
create-object-request;

## FORMATTED PROBLEM STATEMENT

```

160 object-id in the appropriate file based on the value
161 of obj-sec-level.
162 3. Produce an audit incident and generate a decision
163 based on the value of error-code and then terminate.;
164 INCEPTION-CAUSES:
165   init-create-object-procedure;
166   occur-create-object-request;
167 PROCESS
168   create-object-information;
169 DESCRIPTION:
170   This process creates an occurrence of object-
171   information in the appropriate set according to the value
172   of obj-sec-level and sets the value of object-location.;
173 KEYWORDS:
174   low-level;
175   create-object;
176   object-information
177   object-id,
178   obj-sec-level;
179   create-object-information-succ;
180   sub-obj-sec-level-check-succ;
181 TERMINATION-CAUSES:
182   create-subject;
183   cresub;
184 PROCESS
185   SYNONYMS ARE:
186   DESCRIPTION:
187   This process allows the system security
188   administrator with security-id to create the record
189   of a subject with subject-id. This subject will
190   be assigned maximum security level sub-max-sec-level and
191   current security level obj-sec-level.;
192   administrative-security-system;
193   create-subject-response;
194   create-subject-command;
195 PART OP:
196 DERIVES:
197 USES:
198   delete-access-relation;
199 PROCESS
200   DESCRIPTION:
201   This process deletes a subject-access-to-object
202   relation with usage attribute between subject with
203   subject-id and object with object-id.;
204   low-level;
205   release-usage-attr;
206   error-code
207   subject-id,
208   KEYWORDS:
209   UTILIZED BY:
210   DERIVES:
211   USING:

```

## FORMATTED PROBLEM STATEMENT

```

242      base.;
243      PART OF:
244      DERIVES:
245      USES:
246      HAPPENS:
247      number-of-dump-audit TIMES-PER month;
248
249      PROCESS
250      DESCRIPTION:
251          This process derives a decision type based on
252          the value of error-code.;
253      KEYWORDS:
254      UTILIZED BY:
255
256      DERIVES:
257      USING:
258      TRIGGERED BY:
259
260      low-level;
261      get-read;
262      release-usage-attr;
263      create-object;
264      decision-type
265      error-code;
266      need-to-know-check-fails,
267      sub-obj-sec-level-check-fails,
268      create-access-relation-succ,
269      delete-access-relation-succ,
270      access-usage-check-fails,
271      create-object-information-succ;
272
273      PROCESS
274      SYNONYMS ARE:
275      DESCRIPTION:
276
277          This process decides whether or not to enable
278          subject with subject-id execute access to object with
279          object-id. This process is only useful if the
280          object-id requested is a procedure.;
281
282      PART OF:
283      DERIVES:
284      USES:
285      HAPPENS:
286      number-of-dump-audit TIMES-PER month;
287
288      PROCESS
289      DESCRIPTION:
290          This process decides whether or not to enable
291          subject with subject-id read only access to object with
292          object-id.;

```

## FORMATTED PROBLEM STATEMENT

PART OF:  
UTILIZES:

reference-monitor;  
check-need-to-know-usage,  
check-sub-obj-sec-levels,  
create-access-relation,  
produce-audit-incident,  
generate-decision;  
get-read-decision;  
get-read-request;

## DERIVES:

## USES:

## PROCEDURE:

1. Check if subject-need-to-know-object relation exists with usage-attribute value of read between subject with subject-id and object with object-id. If answer is no, go to step 4.
2. Otherwise, check if subject's sub-curr-sec-level exceeds object's obj-sec-level. If answer is no, go to step 4.
3. Otherwise, create a subject-access-to-object relation with usage-attribute between subject with subject-id and object with object-id.
4. Produce an audit incident and generate a decision based on the value of error-code and then terminate.;

## INCEPTION-CAUSES:

## TRIGGERED BY:

## PROCESS

## SYNONYMS ARE:

## DESCRIPTION:

get-read-write;  
kf4;

This process decides whether or not to enable subject with subject-id read and write access to object with object-id.;

## PART OF:

## DERIVES:

## USES:

reference-monitor;  
get-read-write-decision;  
get-read-write-request;

## PROCESS

## SYNONYMS ARE:

## DESCRIPTION:

get-write;  
kf2;

This process decides whether or not to enable subject with subject-id write only access to object with object-id.;

## PART OF:

reference-monitor;

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

324 DERIVES:
325 USES:
326
327 PROCESS
328     SYNONYMS ARE:
329     DESCRIPTION:
330
331         This process decides whether or not subject with
332         requesting-subject-id may give subject with
333         receiving-subject-id usage attribute access to object
334         with object-id.;
335
336     PART OF:
337     DERIVES:
338     USES:
339
340         reference-monitor;
341         give-usage-attr-decision;
342         give-usage-attr-request;
343
344     PROCESS
345     SYNONYMS ARE:
346     DESCRIPTION:
347
348         inc-audit;
349         incaud;
350
351         This process allows the system security
352         administrator obtain all sets of sub-obj-audit-
353         information for a particular incident with incident-
354         type.;
355
356     PART OF:
357     DERIVES:
358     USES:
359
360         auditing-system;
361         inc-audit-trail;
362         inc-audit-request;
363
364     PROCESS
365     SYNONYMS ARE:
366     DESCRIPTION:
367
368         link-reference-monitor;
369         linkrmon;
370
371         This process allows the system security
372         administrator with security-id to perform all
373         reference monitor functions without security checks
374         by the reference monitor. He may perform these
375         functions for any subject-id registered in the system.
376         This process will effectively link the administrative
377         security system to the reference monitor with the only
378         security check being that of the system security
379         administrator's security-id.;
380
381     PART OF:
382     DERIVES:
383     USES:
384
385         administrative-security-system;
386         link-reference-monitor-resp;
387         link-reference-monitor-com1;

```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

365 PROCESS
366     SYNONYMS ARE:
367     DESCRIPTION:
368
369         This process allows the system security
370         administrator obtain all sets of sub-inc-audit-
371         information for a particular object with object-id.;
372
373     PART OF:
374     DERIVES:
375     USES:
376     HAPPENS:
377         number-of-obj-audit TIMES-PER month;
378
379 PROCESS
380     SYNONYMS ARE:
381     DESCRIPTION:
382
383         This process allows the system security
384         administrator obtain all sets of sub-audit-information
385         for a particular object with object-id and incident
386         with incident-id.;
387
388     PART OF:
389     DERIVES:
390     USES:
391         auditing-system;
392         obj-inc-audit-trail;
393         obj-inc-audit-request;
394
395         produce-audit-incident;
396
397 PROCESS
398     DESCRIPTION:
399
400         This process produces an occurrence of incident-
401         information in the auditing system data base based on
402         the value of error-code.;
403
404     KEYWORDS:
405     UTILIZED BY:
406
407         low-level;
408         get-read,
409         release-usage-attr,
410         create-object;
411         incident-information
412         error-code;
413         need-to-know-check-fails,
414         sub-obj-sec-level-check-fails,
415         access-usage-check-fails;
416
417     DERIVES:
418     USING:
419     TRIGGERED BY:
420
421         reference-monitor;
422         access-control-system,
423         rmon;
424
425 PROCESS
426     SYNONYMS ARE:
427     APP:
428
429         reference-monitor;
430         access-control-system,
431         rmon;

```

## FORMATTED PROBLEM STATEMENT

## DESCRIPTION:

The system will provide controls which will allow users to operate concurrently while preventing the release of information to unauthorized users. The system will also prevent inadvertent violation of need to know access to data. In addition to providing the primary access controls for this environment, the system will provide programs which perform subsidiary security control functions.

The capability must be provided for the system hardware to check the validity of all arguments utilized in calling the operating system.;

## KEYWORDS:

## PART OF:

## SUBPARTS ARE:

level-2;  
security-control-system;

get-read,  
get-write,

get-execute,

get-read-write,

release-usage-attr,

give-usage-attr,

rescind-usage-attr,

create-object,

delete-object,

change-sub-curr-sec-level,

change-obj-sec-level;

reference-monitor-request;

reference-monitor-decision;

reference-monitor-decision;

auditing-system-data-base;

reference-monitor-request,

reference-monitor-data-base;

reference-monitor-data-base;

release-usage-attr;

release-usage-attr;

release-usage-attr;

release-usage-attr;

## PROCESS

## SYNONYMS ARE:

## DESCRIPTION:

This process releases usage attribute access to object with object-id from subject with subject-id.;

## PART OF:

## UTILIZES:

reference-monitor;

check-access-usage,

delete-access-relation,

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

## Security-control-example

## FORMATTED PROBLEM STATEMENT

447 DERIVES: produce-audit-incident,  
 448 generate-decision;  
 449 USES: release-usage-attr-decision;  
 450 release-usage-attr-request;  
 451 PROCEDURE:  
 452 1. check if subject-access-to-object relation exists  
 453 with usage-attribute between subject with subject-id  
 454 and object with object-id. If answer is no, go to  
 455 step 3.  
 456 2. Otherwise, delete the relation.  
 457 3. produce an audit incident and generate a decision based  
 458 on the value of error-code and then terminate.;  
 459 INIT-RELEASE-USAGE-ATTR-PROC;  
 460 OCCUR-RELEASE-USAGE-ATTR-REQ;  
 461 TRIGGERED BY:

462 PROCESS rescind-usage-attr;  
 463 SYNONYMS ARE: kf7;  
 464 DESCRIPTION:  
 465 This process decides whether or not subject  
 466 with requesting-subject-id may take usage attribute  
 467 access of object with object-id from subject with  
 468 receiving-subject-id.;  
 469 PART OF:  
 470 DERIVES: reference-monitor;  
 471 USES: rescind-usage-attr-decision;  
 472 rescind-usage-attr-request;

473 PROCESS security-control-system;  
 474 SYNONYMS ARE: SCS,  
 475 SCSYS;  
 476 DESCRIPTION:  
 477 The system will provide a means to allow users to  
 478 process information concurrently while providing  
 479 reasonable assurance that no unauthorized release of  
 480 information shall take place. The security features must  
 481 be an integral part of the operating system. The  
 482 contractor can assume that the physical installation  
 483 will be secured to the highest level of information in  
 484 the system.;

485 SER-MEMO: system-philosophy-memo;  
 486 KEYWORDS: level-1;  
 487 ATTRIBUTES ARE:



## Security-control-example

## FORMATTED PROBLEM STATEMENT

529 DERIVES:  
530 USES:  
531  
532 PROCESS  
533 SYNONYMS ARE:  
534 DESCRIPTION:  
535  
536 This process allows the system security  
537 administrator obtain all sets of audit-information  
538 for a particular subject with subject-id, object with  
539 object-id, and incident with incident-type.:  
540 auditing-system;  
541 sub-obj-inc-audit-trail;  
542 sub-obj-inc-audit-request;  
543 EOF EOF EOF EOF EOF

PART OF:  
DERIVES:  
USES:

sub-obj-inc-audit-trail;  
sub-obj-inc-audit-request;

sub-obj-inc-audit;  
subobjincaud;

## Security-control-example

## OUTPUT STRUCTURE

## PARAMETERS FOR: STR

OUTPUT INDENT=3 NOINDEX

## COUNT LEVEL NAME

```

1 security-control-output
2 reference-monitor-decision
3 get-read-decision
3 get-write-decision
3 get-execute-decision
3 get-read-write-decision
3 release-usage-attr-decision
3 give-usage-attr-decision
3 rescind-usage-attr-decision
3 create-object-decision
3 delete-object-decision
3 change-sub-curr-sec-level-dec
3 change-obj-sec-level-decision
3 administrative-security-resp
2 create-subject-response
3 delete-subject-response
3 change-sub-max-sec-level-resp
3 link-reference-monitor-resp
2 audit-trail
3 sub-obj-audit-trail
3 sub-inc-audit-trail
3 sub-obj-inc-audit-trail
3 sub-audit-trail
3 obj-inc-audit-trail
3 obj-audit-trail
3 inc-audit-trail
3 dump-audit-trail

```

LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT
1	1	2	3
1	2	3	23

## Name Generation

## PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='OUT' ORDER=BY TYPE

1	administrative-security-resp	OUTPUT
2	audit-trail	OUTPUT
3	change-obj-sec-level-decision	OUTPUT
4	change-sub-curr-sec-level-dec	OUTPUT
5	change-sub-max-sec-level-resp	OUTPUT
6	create-object-decision	OUTPUT
7	create-subject-response	OUTPUT
8	delete-object-decision	OUTPUT
9	delete-subject-response	OUTPUT
10	dump-audit-trail	OUTPUT
11	get-execute-decision	OUTPUT
12	get-read-decision	OUTPUT
13	get-read-write-decision	OUTPUT
14	get-write-decision	OUTPUT
15	give-usage-attr-decision	OUTPUT
16	inc-audit-trail	OUTPUT
17	link-reference-monitor-resp	OUTPUT
18	obj-audit-trail	OUTPUT
19	obj-inc-audit-trail	OUTPUT
20	reference-monitor-decision	OUTPUT
21	release-usage-attr-decision	OUTPUT
22	rescind-usage-attr-decision	OUTPUT
23	security-control-output	OUTPUT
24	sub-audit-trail	OUTPUT
25	sub-inc-audit-trail	OUTPUT
26	sub-obj-audit-trail	OUTPUT
27	sub-obj-inc-audit-trail	OUTPUT

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=7) CMARG=1 HMARG=40 DPSG  
 ONE-PER-LINE DEFINE COMMENT NONNEW-PAGE NONNEW-LINE

1 OUTPUT administrative-security-resp;  
 2 SYNONYMS ARE: admsres;  
 3 DESCRIPTION;

4 These are responses to administrative security  
 5 commands and will consist of validations as to  
 6 the execution of these commands.;

7 KEYWORDS: level-2;  
 8 PART OF: security-control-output;  
 9 SUBPARTS ARE: create-subject-response,  
 10 delete-subject-response,  
 11 change-sub-max-sec-level-resp,  
 12 link-reference-monitor-resp;  
 13 DERIVED BY: administrative-security-system;  
 14 GENERATED BY: administrative-security-system;  
 15 RECEIVED BY: system-security-administrator;  
 16

17 OUTPUT audit-trail;  
 18 SYNONYMS ARE: audtra;  
 19 DESCRIPTION;

20 Security audit trails should contain records of  
 21 each security incident, and may contain other data  
 22 as well.;

23 KEYWORDS: level-2;  
 24 PART OF: security-control-output;  
 25 SUBPARTS ARE: sub-obj-audit-trail,  
 26 sub-inc-audit-trail,  
 27 sub-obj-inc-audit-trail,  
 28 sub-audit-trail,  
 29 obj-inc-audit-trail,  
 30 obj-audit-trail,  
 31 inc-audit-trail,  
 32 dump-audit-trail;  
 33 DERIVED BY: auditing-system;  
 34 GENERATED BY: auditing-system;  
 35 RECEIVED BY: system-security-administrator;  
 36

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```
37 OUTPUT
38 SYNONYMS ARE:
39 PART OF:
40 CONSISTS OF:
41
42 DERIVED BY:
43
44 OUTPUT
45 SYNONYMS ARE:
46 PART OF:
47 CONSISTS OF:
48
49 DERIVED BY:
50
51 OUTPUT
52 SYNONYMS ARE:
53 PART OF:
54 CONSISTS OF:
55
56 DERIVED BY:
57
58 OUTPUT
59 SYNONYMS ARE:
60 PART OF:
61 CONSISTS OF:
62
63 DERIVED BY:
64
65 OUTPUT
66 SYNONYMS ARE:
67 PART OF:
68 CONSISTS OF:
69
70 DERIVED BY:
71
72 OUTPUT
73 SYNONYMS ARE:
74 PART OF:
75 CONSISTS OF:
76
77 DERIVED BY:
```

change-obj-sec-level-decision;  
kf11dec;  
reference-monitor-decision;  
  
decision-type;  
change-obj-sec-level;  
  
change-sub-curr-sec-level-dec;  
kf10dec;  
reference-monitor-decision;  
  
decision-type;  
change-sub-curr-sec-level;  
  
change-sub-max-sec-level-resp;  
chasubmaxseclvres;  
administrative-security-resp;  
  
validation-code;  
change-sub-max-sec-level;  
  
create-object-decision;  
kf8dec;  
reference-monitor-decision;  
  
decision-type;  
create-object;  
  
create-subject-response;  
cresubres;  
administrative-security-resp;  
  
validation-code;  
create-subject;  
  
delete-object-decision;  
kf9dec;  
reference-monitor-decision;  
  
decision-type;  
delete-object;

AD-A065 948

MICHIGAN UNIV ANN ARBOR DEPT OF INDUSTRIAL AND OPERA--ETC F/G 5/9  
URL/URA TRAINING EXAMPLE.(U)  
DEC 78

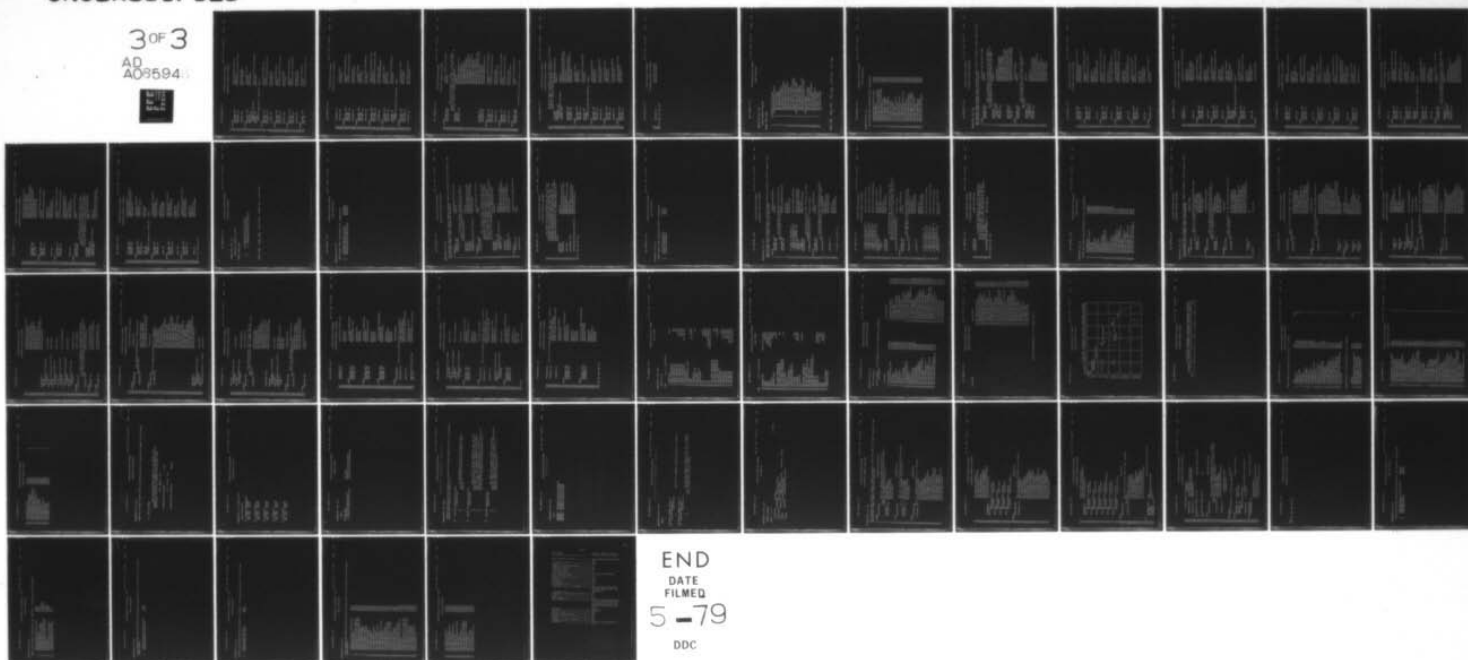
UNCLASSIFIED

ESD-TR-78-126

F19628-76-C-0197  
NL

3 OF 3

AD  
A06594



END  
DATE  
FILMED  
5-79  
DDC



## FORMATTED PROBLEM STATEMENT

```
78
79 OUTPUT
80 SYNONYMS ARE:
81 PART OF:
82 CONSISTS OF:
83
84 DERIVED BY:
85
86 OUTPUT
87 SYNONYMS ARE:
88 PART OF:
89 CONSISTS OF:
90 number-of-incidents
91 DERIVED BY:
92 HAPPENS:
93 number-of-dump-audit TIMES-PER
94 month;
95 OUTPUT
96 SYNONYMS ARE:
97 PART OF:
98 CONSISTS OF:
99
100 DERIVED BY:
101
102 OUTPUT
103 SYNONYMS ARE:
104 PART OF:
105 CONSISTS OF:
106
107 DERIVED BY:
108
109 OUTPUT
110 SYNONYMS ARE:
111 PART OF:
112 CONSISTS OF:
113
114 DERIVED BY:
115
116 OUTPUT
117 SYNONYMS ARE:
118 PART OF:

delete-subject-response;
delsubres;
administrative-security-resp;

validation-code;
delete-subject;

dump-audit-trail;
dumaudtra;
audit-trail;

sub-obj-inc-audit-information;
dump-audit;

get-execute-decision;
kf3dec;
reference-monitor-decision;

decision-type;
get-execute;

get-read-decision;
kf11dec;
reference-monitor-decision;

decision-type;
get-read;

get-read-write-decision;
kf41dec;
reference-monitor-decision;

decision-type;
get-read-write;

get-write-decision;
kf2dec;
reference-monitor-decision;
```

FORMATTED PROBLEM STATEMENT

```

119 CONSISTS OF:
120
121 DERIVED BY:
122
123 OUTPUT
124 SYNONYMS ARE:
125 PART OF:
126 CONSISTS OF:
127
128 DERIVED BY:
129
130 OUTPUT
131 SYNONYMS ARE:
132 PART OF:
133 CONSISTS OF:
134
135 DERIVED BY:
136
137 OUTPUT
138 SYNONYMS ARE:
139 PART OF:
140 CONSISTS OF:
141
142 DERIVED BY:
143
144 OUTPUT
145 SYNONYMS ARE:
146 PART OF:
147 CONSISTS OF:
148
149 DERIVED BY:
150 HAPPENS:
151 number-of-obj-audit TIMES-PER
152 month;
153 OUTPUT
154 SYNONYMS ARE:
155 PART OF:
156 CONSISTS OF:
157
158 DERIVED BY:
159

```

decision-type;  
 get-write;  
  
 give-usage-attr-decision;  
 kf6dec;  
 reference-monitor-decision;  
  
 decision-type;  
 give-usage-attr;  
  
 inc-audit-trail;  
 incaudtra;  
 audit-trail;  
  
 sub-obj-audit-information;  
 inc-audit;  
  
 link-reference-monitor-resp;  
 linkmonres;  
 administrative-security-resp;  
  
 validation-code;  
 link-reference-monitor;  
  
 obj-audit-trail;  
 objaudtra;  
 audit-trail;  
  
 sub-inc-audit-information;  
 obj-audit;  
  
 obj-inc-audit-trail;  
 objincaudtra;  
 audit-trail;  
  
 sub-audit-information;  
 obj-inc-audit;

## FORMATTED PROBLEM STATEMENT

```

160 OUTPUT
161 SYNONYMS ARE:
162 DESCRIPTION;
163
164     These are decisions in answer to the reference
165     monitor subject's request and allow for read, write, or
166     execute access to system information.;
167
168 KEYWORDS:
169 PART OF:
170 SUBPARTS ARE:
171
172     reference-monitor-decision;
173     rmondec;
174
175     level-2;
176     security-control-output;
177     get-read-decision,
178     get-write-decision,
179     get-execute-decision,
180     get-read-write-decision,
181     release-usage-attr-decision,
182     give-usage-attr-decision,
183     rescind-usage-attr-decision,
184     create-object-decision,
185     delete-object-decision,
186     change-sub-curr-sec-level-dec,
187     change-obj-sec-level-decision;
188     reference-monitor;
189     reference-monitor;
190     reference-monitor-subject;
191
192     release-usage-attr-decision;
193     kf5dec;
194     reference-monitor-decision;
195
196     decision-type;
197     release-usage-attr;
198
199     rescind-usage-attr-decision;
200     kf7dec;
201     reference-monitor-decision;
202
203     decision-type;
204     rescind-usage-attr;
205
206     security-control-output;
207     scout;
208
209     The system will produce outputs of several
210

```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

201 different types: approvals to data access or modification  
 202 requests, audit trails on security features, a  
 203 record of outputs produced, etc.;

204 SEE-MEMO: system-philosophy-memo;  
 205 KEYWORDS: level-1;

206 ATTRIBUTES ARE:  
 207 specification-derivation  
 208 SUBPARTS ARE:  
 209  
 210 implicit;  
 211 reference-monitor-decision,  
 212 administrative-security-resp,  
 213 audit-trail;  
 214 security-control-system;  
 215 security-control-interface;  
 216 unclassified;

217 OUTPUT  
 218 SYNONYMS ARE:  
 219 PART OF:  
 220 CONSISTS OF:  
 221  
 222 DERIVED BY:  
 223 HAPPENS:  
 224 number-of-sub-audit TIMES-PER  
 225 month;

226 sub-audit-trail;  
 227 subaudtra;  
 228 audit-trail;  
 229  
 230 obj-inc-audit-information;  
 231 sub-audit;

232 sub-inc-audit-trail;  
 233 subincaudtra;  
 234 audit-trail;  
 235  
 236 obj-audit-information;  
 237 sub-inc-audit;

238 sub-obj-audit-trail;  
 239 subobjaudtra;  
 240 audit-trail;  
 241  
 242 inc-audit-information;  
 243 sub-obj-audit;

244 sub-obj-inc-audit-trail;  
 245 subobjincaudtra;  
 246 audit-trail;

Security-control-example

FORMATTED PROBLEM STATEMENT

audit-information;  
sub-obj-inc-audit;

242  
243 DERIVED BY:  
244  
245 EOF EOF EOF EOF

## INPUT STRUCTURE

## PARAMETERS FOR: STR

INPUT INDENT=3 NOINDEX

## COUNT LEVEL NAME

1	1	security-control-input
2	2	reference-monitor-request
3	3	get-read-request
4	3	get-write-request
5	3	get-execute-request
6	3	get-read-write-request
7	3	release-usage-attr-request
8	3	give-usage-attr-request
9	3	rescind-usage-attr-request
10	3	create-object-request
11	3	delete-object-request
12	3	change-sub-curr-sec-level-req
13	3	change-obj-sec-level-request
14	2	administrative-security-command
15	3	create-subject-command
16	3	delete-subject-command
17	3	change-sub-max-sec-level-command
18	3	link-reference-monitor-command
19	2	auditing-request
20	3	sub-obj-audit-request
21	3	sub-inc-audit-request
22	3	sub-obj-inc-audit-request
23	3	sub-audit-request
24	3	obj-inc-audit-request
25	3	obj-audit-request
26	3	inc-audit-request
27	3	dump-audit-request

LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT
1	2	3	23
1	1	3	3

## Security-control-example

## Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='INP' ORDER=BYTYPE

1	administrative-security-comd	INPUT
2	auditing-request	INPUT
3	change-obj-sec-level-request	INPUT
4	change-sub-curr-sec-level-req	INPUT
5	change-sub-max-sec-level-comd	INPUT
6	create-object-request	INPUT
7	create-subject-command	INPUT
8	delete-object-request	INPUT
9	delete-subject-command	INPUT
10	dump-audit-request	INPUT
11	get-execute-request	INPUT
12	get-read-request	INPUT
13	get-read-write-request	INPUT
14	get-write-request	INPUT
15	give-usage-attr-request	INPUT
16	inc-audit-request	INPUT
17	link-reference-monitor-comd	INPUT
18	obj-audit-request	INPUT
19	obj-inc-audit-request	INPUT
20	reference-monitor-request	INPUT
21	release-usage-attr-request	INPUT
22	rescind-usage-attr-request	INPUT
23	security-control-input	INPUT
24	sub-audit-request	INPUT
25	sub-inc-audit-request	INPUT
26	sub-obj-audit-request	INPUT
27	sub-obj-inc-audit-request	INPUT

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=7) CMARG=1 HMARG=40 DESG  
 ONE-PER-LINE DEFINE COMMENT NONFW-PAGE NONFW-LINE

1 INPUT administrative-security-comd;  
 2 SYNONYMS ARE:  
 3 admscom;  
 4 DESCRIPTION;

5 These are commands necessary to the performance  
 6 of administrative security functions and will allow for  
 7 the maintenance of the reference monitor data base.;  
 8 level-2;

9 KEYWORDS:  
 10 ATTRIBUTES ARE:  
 11 occurrences

12 PART OF:  
 13 SUBPARTS ARE:

14 unscheduled;  
 15 security-control-input;  
 16 create-subject-command,  
 17 delete-subject-command,  
 18 change-sub-max-sec-level-comd,  
 19 link-reference-monitor-comd;  
 20 system-security-administrator;  
 21 administrative-security-system;  
 22 administrative-security-system;

23 INPUT auditing-request;  
 24 audreq;  
 25 DESCRIPTION;

26 These are requests to view audit data stored in  
 27 the auditing system data base by the reference  
 28 monitor.;

29 KEYWORDS:  
 30 ATTRIBUTES ARE:  
 31 occurrences  
 32 PART OF:  
 33 SUBPARTS ARE:

34 level-2;  
 35 scheduled;  
 36 security-control-input;  
 37 sub-obj-audit-request,  
 38 sub-inc-audit-request,  
 39 sub-obj-inc-audit-request,  
 40 sub-audit-request,  
 41 obj-inc-audit-request,  
 42 obj-audit-request,  
 43 inc-audit-request,  
 44 dump-audit-request;

## FORMATTED PROBLEM STATEMENT

```

37  GENERATED BY:
38  RECEIVED BY:
39  USED BY:
40
41  INPUT
42  SYNONYMS ARE:
43  PART OF:
44  CONSISTS OF:
45
46
47
48
49
50  INPUT
51  SYNONYMS ARE:
52  PART OF:
53  CONSISTS OF:
54
55
56
57  USED BY:
58
59  INPUT
60  SYNONYMS ARE:
61  PART OF:
62  CONSISTS OF:
63
64
65
66  USED BY:
67  INPUT
68  SYNONYMS ARE:
69  PART OF:
70  CONSISTS OF:
71
72
73
74  USED BY:
75
76  INPUT
77  SYNONYMS ARE:

system-security-administrator;
auditing-system;
auditing-system;

change-obj-sec-level-request;
kf11req;
reference-monitor-request;

subject-id,
object-id,
obj-sec-level;
change-obj-sec-level;

change-sub-curr-sec-level-req;
kf10req;
reference-monitor-request;

subject-id,
sub-curr-sec-level;
change-sub-curr-sec-level;

change-sub-max-sec-level-com1;
chasubmaxseclevcom;
administrative-security-com1;

security-id,
subject-id,
sub-max-sec-level;
change-sub-max-sec-level;

create-object-request;
kf8req;
reference-monitor-request;

subject-id,
object-id,
obj-sec-level;
create-object;

create-subject-command;
cresubcom;

```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

78 PART OF:
79 CONSISTS OF:
80
81 security-id,
82 subject-id,
83 sub-max-sec-level,
84 sub-curr-sec-level;
85 create-subject;
86
87 INPUT
88 SYNONYMS ARE:
89 PART OF:
90 CONSISTS OF:
91
92 delete-object-request;
93 kf9req;
94 reference-monitor-request;
95
96 subject-id,
97 object-id;
98 delete-object;
99
100 delete-subject-command;
101 delsubcom;
102 administrative-security-com1;
103
104 security-id,
105 subject-id;
106 delete-subject;
107
108 dump-audit-request;
109 dumaudreq;
110 auditing-request;
111 dump-audit;
112
113 number-of-dump-audit TIMES-PER month;
114
115 get-execute-request;
116 kf3req;
117 reference-monitor-request;
118
119 subject-id,
120 object-id,
121 usage-attribute;
122 get-execute;
123
124 get-read-request;

```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

119 SYNONYMS ARE:
120 PART OF:
121 CONSISTS OF:
122
123
124
125
126 USED BY:
127 INPUT
128 SYNONYMS ARE:
129 PART OF:
130 CONSISTS OF:
131
132
133
134 USED BY:
135
136 INPUT
137 SYNONYMS ARE:
138 PART OF:
139 CONSISTS OF:
140
141
142
143 USED BY:
144
145 INPUT
146 SYNONYMS ARE:
147 PART OF:
148 CONSISTS OF:
149
150
151
152 USED BY:
153
154 INPUT
155 SYNONYMS ARE:
156 PART OF:
157 CONSISTS OF:
158
159
kf1req;
reference-monitor-request;

subject-id,
object-id,
usage-attribute;
get-read;

get-read-write-request;
kf4req;
reference-monitor-request;

subject-id,
object-id,
usage-attribute;
get-read-write;

get-write-request;
kf2req;
reference-monitor-request;

subject-id,
object-id,
usage-attribute;
get-write;

give-usage-attr-request;
kf6req;
reference-monitor-request;

requesting-subject-id,
receiving-subject-id,
object-id,
usage-attribute;
give-usage-attr;

inc-audit-request;
incaudreq;
auditing-request;

incident-type;

```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

160 USED BY:
161
162 INPUT
163     SYNONYMS ARE:
164     PART OF:
165     CONSISTS OF:
166
167 USED BY:
168
169 INPUT
170     SYNONYMS ARE:
171     PART OF:
172     CONSISTS OF:
173
174 USED BY:
175 HAPPENS:
176     number-of-obj-audit TIMES-PER
177     month:
178
179 INPUT
180     SYNONYMS ARE:
181     PART OF:
182     CONSISTS OF:
183
184 USED BY:
185
186 INPUT
187     SYNONYMS ARE:
188     DESCRIPTION:
189
190     These are requests to access or modify information
191     in the system and may include output options.:
192
193     KEYWORDS:
194     ATTRIBUTES ARE:
195     OCCURRENCES
196     PART OF:
197     SUBPARTS ARE:
198
199     inc-audit;
200     link-reference-monitor-comd;
    linkmoncom;
    administrative-security-comd;
    security-id;
    link-reference-monitor;
    obj-audit-request;
    objaudreq;
    auditing-request;
    object-id;
    obj-audit;
    obj-inc-audit-request;
    objincaudreq;
    auditing-request;
    object-id,
    incident-type;
    obj-inc-audit;
    reference-monitor-request;
    rmonreq;
    unscheduled;
    security-control-input;
    get-read-request,
    get-write-request,
    get-execute-request,
    get-read-write-request,
    release-usage-attr-request,
    give-usage-attr-request,

```

## Security-control-example

## FORMATTED PROBLEM STATEMENT

201 rescind-usage-attr-request,  
 202 create-object-request,  
 203 delete-object-request,  
 204 change-sub-curr-sec-level-req,  
 205 change-obj-sec-level-request;  
 206 reference-monitor-subject;  
 207 reference-monitor;  
 208 reference-monitor;  
 209  
 210 INPUT  
 211 SYNONYMS ARE:  
 212 PART OF:  
 213 CONSISTS OF:  
 214  
 215  
 216  
 217  
 218  
 219 INPUT  
 220 SYNONYMS ARE:  
 221 PART OF:  
 222 CONSISTS OF:  
 223  
 224  
 225  
 226  
 227  
 228  
 229 INPUT  
 230 SYNONYMS ARE:  
 231 DESCRIPTION:  
 232  
 233 The input to the security control system  
 234 consists of requests by users to access and  
 235 modify information in the system and of commands  
 236 by security personnel to monitor the system;  
 237 system-philosophy-memo;  
 238 level-1;  
 239 implicit;  
 240 reference-monitor-request,  
 241 administrative-security-command,

## FORMATTED PROBLEM STATEMENT

242           GENERATED BY:  
243           RECEIVED BY:  
244           SECURITY IS:  
245  
246  
247       INPUT  
248           SYNONYMS ARE:  
249           PART OF:  
250           CONSISTS OF:  
251  
252       USED BY:  
253       HAPPENS:  
254       number-of-sub-audit TIMES-PER  
255       month:  
256       INPUT  
257           SYNONYMS ARE:  
258           PART OF:  
259           CONSISTS OF:  
260  
261       USED BY:  
262  
263       INPUT  
264           SYNONYMS ARE:  
265           PART OF:  
266           CONSISTS OF:  
267  
268       USED BY:  
269  
270       INPUT  
271           SYNONYMS ARE:  
272           PART OF:  
273           CONSISTS OF:  
274  
275       USED BY:  
276  
277       INPUT  
278           SYNONYMS ARE:  
279           PART OF:  
280           CONSISTS OF:  
281       USED BY:

auditing-request;  
security-control-interface;  
security-control-system;  
unclassified;

sub-audit-request;  
subaudreq;  
auditing-request;  
subject-id;  
sub-audit;

sub-inc-audit-request;  
subincaudreq;  
auditing-request;  
subject-id,  
incident-type;  
sub-inc-audit;

sub-obj-audit-request;  
subobjaudreq;  
auditing-request;  
subject-id,  
object-id;  
sub-obj-audit;

sub-obj-inc-audit-request;  
subobjincaudreq;  
auditing-request;  
subject-id,  
object-id,  
incident-type;  
sub-obj-inc-audit;

281 TOP EOP EOP EOP EOP

Security-control-example

INTERFACE STRUCTURE

PARAMETERS FOR: STR

INTERFACE INDENT=3 NOINDEX

COUNT LEVEL NAME

- 1 security-control-interface
- 2 reference-monitor-subject
- 3 system-security-administrator

LEVEL COUNT	LEVEL COUNT	LEVEL COUNT	LEVEL COUNT
1	1	2	2

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='INTF' ORDER=BYTYPE

- |   |                               |           |
|---|-------------------------------|-----------|
| 1 | reference-monitor-subject     | INTERFACE |
| 2 | security-control-interface    | INTERFACE |
| 3 | system-security-administrator | INTERFACE |

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=79 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONFW-PAGE NONFW-LINE

1 INTERFACE  
2 SYNONYMS ARE:  
3 DESCRIPTION:  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36

A reference monitor subject may be a user, a  
process, or a job which generates requests on the  
reference monitor.;

KEYWORDS:  
PART OF:  
GENERATES:  
RECEIVES:  
RESPONSIBLE-PROBLEM-DEFINER IS:  
level-2;  
security-control-interface;  
reference-monitor-request;  
reference-monitor-decision;  
james-m-amster;

INTERFACE  
SYNONYMS ARE:  
DESCRIPTION:  
security-control-interface;  
scint;

There will be several different types of users  
generating requests on the system and retrieving  
data from it. The security controls of the system  
must be capable of allowing users of different  
authorizations to process concurrently while preventing  
the release of information to unauthorized users.;

SEE-MEMO:  
KEYWORDS:  
ATTRIBUTES ARE:  
SUBPARTS ARE:  
system-philosophy-memo;  
level-1;

specification-derivation  
GENERATES:  
RECEIVES:  
RESPONSIBLE FOR:  
SECURITY IS:  
explicit;  
reference-monitor-subject,  
system-security-administrator;  
security-control-input;  
security-control-output;  
security-control-data-base;  
unclassified;

INTERFACE  
SYNONYMS ARE:  
DESCRIPTION:  
system-security-administrator;  
ssa,  
ssadm;

## FORMATTED PROBLEM STATEMENT

37       The system security administrator will have the  
38       responsibility of receiving and reviewing audit data  
39       contained in the auditing system data base and  
40       performing administrative functions dealing with the  
41       initiation and maintenance of system subject and object  
42       information contained in the reference monitor data  
43       base.;

## KEYWORDS:

PART OF:

GENERATES:

RECEIVES:

RESPONSIBLE FOR:

RESPONSIBLE-PROBLEM-DEFINER IS:

level-2;

security-control-interface;

administrative-security-comd,

auditing-request;

administrative-security-resp,

audit-trail;

reference-monitor-data-base,

auditing-system-data-base;

michel-j-bastarache;

53       EOF EOF EOF EOF EOF

54       EOF EOF EOF EOF EOF

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ENTITY' ORDER=BYTYPE

- 1 incident-information
- 2 object-information
- 3 subject-information

ENTITY  
ENTITY  
ENTITY

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: PPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 VMARG=39 AMARG=7 BMARG=39 RMARG=70 CMARG=1 HMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONEX-PAGE NONEX-LINE

```

1 ENTITY
2 SYNONYMS ARE:
3 DESCRIPTION:
4
5 This information holds data about where and
6 when an incident has occurred.;
7 CONTAINED IN:
8 auditing-system-data-base;
9 CONSISTS OF:
10
11 date-time,
12 consol-nr,
13 incident-type;
14
15 sub-inc-audit-relation;
16
17 obj-inc-audit-relation;
18 produce-audit-incident
19 error-code;
20 number-of-incidents;
21
22 The contents of this type of entity are never
23 changed after creation.;
24 RESPONSIBLE-PROBLEM-DEFINER IS: james-m-amster;
25
26 object-information;
27 objinfo;
28
29 This information holds identification, security,
30 and location information for a particular object.;
31 top-secret-file,
32 secret-file,
33 confidential-file,
34 unclassified-file;
35
36 object-id,
37 obj-sec-level,
38 object-location;
39
40 /* RIGHT */ RELATED TO:
41 subject-information VIA
42 /* RIGHT */ RELATED TO:
43 object-information VIA
44 DERIVED BY:
45 USING:
46 OCCURRENCES:
47 VOLATILITY;
48
49 The contents of this type of entity are never
50 changed after creation.;
51 RESPONSIBLE-PROBLEM-DEFINER IS: james-m-amster;
52
53 object-information;
54 objinfo;
55
56 This information holds identification, security,
57 and location information for a particular object.;
58 top-secret-file,
59 secret-file,
60 confidential-file,
61 unclassified-file;
62
63 object-id,
64 obj-sec-level,
65 object-location;
66
67 /* LEFT */ RELATED TO:

```

FORMATTED PROBLEM STATEMENT

```

37 incident-information VIA
38 /* RIGHT */ RELATED TO:
39 subject-information VIA
40 /* RIGHT */ RELATED TO:
41 subject-information VIA
42 /* RIGHT */ RELATED TO:
43 subject-information VIA
44 IDENTIFIED BY:
45 DERIVED BY:
46 USING:
47
48 OCCURRENCES:
49 VOLATILITY:
50
51 The obj-sec-level may be changed by either the
52 owner of the object or the system security administrator.
53 Changing the object-location is done based on need by
54 the operating system.;
55 RESPONSIBLE-PROBLEM-DEFINER IS: james-m-amster;

```

```

56 ENTITY
57   SYNONYMS ARE:
58   DESCRIPTION:
59     This information holds identification and
60     security data about a reference monitor subject.;
61   CONTAINED IN:
62     top-secret-file,
63     secret-file,
64     confidential-file,
65     unclassified-file;
66
67   CONSISTS OF:
68     subject-id,
69     sub-max-sec-level,
70     sub-curr-sec-level;
71
72   IDENTIFIED BY:
73     subject-access-to-object;
74     subject-need-to-know-object;
75     sub-inc-audit-relation;
76     sub-obj-audit-relation;
77     subject-id;

```

Security-control-example

FORMATTED PROBLEM STATEMENT

78 OCCURRENCES:  
 79 VOLATILITY:  
 80                   The sub-max-sec-level can only be changed by a  
 81                   system security administrator and only on decision  
 82                   of the administrator. The sub-curr-sec-level may  
 83                   change several times within the course of one session  
 84                   on the system.;  
 85                   RESPONSIBLE-PROBLEM-DEFINER IS: james-m-amster;  
 86  
 87 EOF EOF EOF EOF EOF

## Security-control-example

## Name Generation

## PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='GROUP OR FILE' ORDER=BYTYPE

1	category-set	ELEMENT
2	classification-level	ELEMENT
3	consol-nr	ELEMENT
4	date-time	ELEMENT
5	decision-type	ELEMENT
6	error-code	ELEMENT
7	incident-type	ELEMENT
8	object-id	ELEMENT
9	object-location	ELEMENT
10	receiving-subject-id	ELEMENT
11	requesting-subject-id	ELEMENT
12	security-id	ELEMENT
13	subject-id	ELEMENT
14	usage-attribute	ELEMENT
15	validation-code	ELEMENT
16	audit-information	GROUP
17	inc-audit-information	GROUP
18	obj-audit-information	GROUP
19	obj-inc-audit-information	GROUP
20	obj-sec-level	GROUP
21	sub-audit-information	GROUP
22	sub-curr-sec-level	GROUP
23	sub-inc-audit-information	GROUP
24	sub-max-sec-level	GROUP
25	sub-obj-audit-information	GROUP
26	sub-obj-inc-audit-information	GROUP

## FORMATTED PROBLEM STATEMENT

## PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RMARG=70 CMARG=1 HMARG=40 DESG  
 ONE-PER-LINE DEFINE COMMENT NONEX-PAGE NONEX-LINE

1	ELEMENT	category-set;
2	DESCRIPTION;	
3		This is a set of categories of information which
4		may be owned by a subject or an object.;
5	SEE-MEMO:	category-set-memo;
6	CONTAINED IN:	sub-max-sec-level,
7		sub-curr-sec-level,
8		obj-sec-level;
9		
10	ELEMENT	classification-level;
11	DESCRIPTION;	
12		This is a level of classification which may
13		range up from unclassified to top secret and may be
14		owned by a subject or an object.;
15	SEE-MEMO:	clearance-memo;
16	CONTAINED IN:	sub-max-sec-level,
17		sub-curr-sec-level,
18		obj-sec-level;
19		
20	ELEMENT	console-nr;
21	DESCRIPTION;	
22		This is the number of the console at which the audit
23		incident occurred.;
24	CONTAINED IN:	
25		incident-information,
26		inc-audit-information,
27		obj-audit-information,
28		audit-information,
29		obj-inc-audit-information,
30		sub-audit-information,
31		sub-inc-audit-information,
32		sub-obj-audit-information,
33		sub-obj-inc-audit-information;
34	VALUES ARE:	
35	0 THRU	25;
36	ELEMENT	date-time;

## FORMATTED PROBLEM STATEMENT

37 DESCRIPTION: This is the date and time an audit incident  
38 occurred.;  
39 CONTAINED IN:  
40 incident-information,  
41 inc-audit-information,  
42 obj-audit-information,  
43 audit-information,  
44 obj-inc-audit-information,  
45 sub-audit-information,  
46 sub-inc-audit-information,  
47 sub-obj-audit-information,  
48 sub-obj-inc-audit-information;  
49  
50 ELEMENT decision-type;  
51 DESCRIPTION: This is the affirmative or negative decision to  
52 a subject's request.;  
53 CONTAINED IN:  
54 get-read-decision,  
55 get-write-decision,  
56 get-execute-decision,  
57 get-read-write-decision,  
58 release-usage-attr-decision,  
59 give-usage-attr-decision,  
60 rescind-usage-attr-decision,  
61 create-object-decision,  
62 delete-object-decision,  
63 change-sub-curr-sec-level-dec,  
64 change-obj-sec-level-decision;  
65 generate-decision  
66 error-code;  
67  
68 ELEMENT error-code;  
69 check-need-to-know-usage  
70 subject-id,  
71 object-id,  
72 usage-attribute;  
73 check-sub-obj-sec-levels  
74 sub-curr-sec-level,  
75 obj-sec-level;  
76 check-access-usage  
77 subject-id,

## FORMATTED PROBLEM STATEMENT

```

78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118

DERIVED BY:
  USING:
    object-id,
    usage-attribute;
    delete-access-relation
    subject-id,
    object-id;
    delete-object-information
    object-id,
    obj-sec-level;

USED BY:
  produce-audit-incident
  TO DERIVE
    incident-information;

USED BY:
  generate-decision TO DERIVE
    decision-type;
    incident-type;

DESCRIPTION:
  This specifies the type of audit incident which
  has occurred.;

CONTAINED IN:
  incident-information,
  inc-audit-information,
  sub-inc-audit-request,
  sub-obj-inc-audit-request,
  obj-inc-audit-information,
  obj-inc-audit-request,
  sub-inc-audit-information,
  inc-audit-request,
  sub-obj-inc-audit-information;

ELEMENT
DESCRIPTION:
  object-id;

CONTAINED IN:
  This is a unique identifier for an object.;
  object-information,
  get-read-request,
  get-write-request,
  get-execute-request,
  get-read-write-request,
  release-usage-attr-request,
  give-usage-attr-request,
  rescind-usage-attr-request,
  create-object-request,
  delete-object-request,

```

## FORMATTED PROBLEM STATEMENT

```

119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
IDENTIFIERS:
USED BY:
  check-need-to-know-usage
    TO DERIVE
USED BY:
  check-access-usage TO DERIVE
USED BY:
  delete-access-relation
    TO DERIVE
USED BY:
  create-object-information
    TO DERIVE
USED BY:
  delete-object-information
    TO DERIVE
USED BY:
  create-access-relation
    TO UPDATE
ELEMENT
DESCRIPTION:
  This is a pointer to the actual object which
  contains the information of interest to a subject and
  which exists outside the security control system.;
CONTAINED IN:
  object-information;
ELEMENT
CONTAINED IN:
  receiving-subject-id;
  give-usage-attr-request;
  rescind-usage-attr-request;
ELEMENT
CONTAINED IN:
  requesting-subject-id;
  give-usage-attr-request;

```

change-obj-sec-level-request,  
sub-obj-audit-request,  
obj-audit-information,  
sub-obj-inc-audit-request,  
obj-inc-audit-information,  
obj-inc-audit-request,  
obj-audit-request,  
sub-obj-audit-information,  
sub-obj-inc-audit-information;  
object-information;

error-code;  
error-code;  
error-code;

object-information;  
error-code;  
usage-attribute;  
object-location;

## Security-control-example

## FORMATTED PROBLEM STATEMENT

160  
161  
162 ELEMENT  
163 DESCRIPTION;  
164 This uniquely identifies the system security  
165 administrator.;  
166 CONTAINED IN:  
167 create-subject-command,  
168 delete-subject-command,  
169 change-sub-max-sec-level-command,  
170 link-reference-monitor-command;

rescind-usage-attr-request;

security-id;

171 ELEMENT  
172 DESCRIPTION;  
173 This is a unique identifier for a subject.;  
174 subject-information,  
175 get-read-request,  
176 get-write-request,  
177 get-execute-request,  
178 get-read-write-request,  
179 release-usage-attr-request,  
180 create-object-request,  
181 delete-object-request,  
182 change-sub-curr-sec-level-request,  
183 change-obj-sec-level-request,  
184 create-subject-command,  
185 delete-subject-command,  
186 change-sub-max-sec-level-command,  
187 sub-obj-audit-request,  
188 sub-inc-audit-request,  
189 sub-obj-inc-audit-request,  
190 sub-audit-request,  
191 sub-audit-information,  
192 sub-inc-audit-information,  
193 sub-obj-audit-information,  
194 sub-obj-inc-audit-information;  
195 subject-information;

subject-id;

IDENTIFIES:

USED BY:

check-need-to-know-usage  
TO DERIVE

USED BY:

check-access-usage TO DERIVE

error-code;

error-code;

## FORMATTED PROBLEM STATEMENT

201 USED BY:  
 202 delete-access-relation  
 203 TO DERIVE  
 204 USED BY:  
 205 create-access-relation  
 206 TO UPDATE  
 207  
 208 ELEMENT  
 209 DESCRIPTION:  
 210 This specifies the type of usage, that is  
 211 read, write, or execute, that a subject may have of an  
 212 object.;  
 213 CONTAINED IN:  
 214 get-read-request,  
 215 get-write-request,  
 216 get-execute-request,  
 217 release-usage-attr-request,  
 218 give-usage-attr-request,  
 219 rescind-usage-attr-request,  
 220 subject-access-to-object,  
 221 subject-need-to-know-object;  
 222  
 223 ASSOCIATED WITH:  
 224  
 225 USED BY:  
 226 check-need-to-know-usage  
 227 TO DERIVE  
 228 USED BY:  
 229 check-access-usage TO DERIVE  
 230 UPDATING BY:  
 231 USING:  
 232  
 233 ELEMENT  
 234 DESCRIPTION:  
 235 This is a validation of a command issued by  
 236 the system security administrator.;  
 237 CONTAINED IN:  
 238 create-subject-response,  
 239 delete-subject-response,  
 240 change-sub-max-sec-level-resp,  
 241 link-reference-monitor-resp;  
 242  
 243 GROUP  
 244 SYNONYMS ARE:  
 245 audit-information;  
 246 audinfo;

error-code;

usage-attribute;

usage-attribute;

error-code;

 error-code;  
 create-access-relation  
 subject-id,  
 object-id;

validation-code;

 audit-information;  
 audinfo;

## Security-control-example

## FORMATTED PROBLEM STATEMENT

242 CONTAINED IN:  
243 CONSISTS OF:  
244  
245  
246  
247 GROUP  
248 SYNONYMS ARE:  
249 CONTAINED IN:  
250 CONSISTS OF:  
251  
252  
253  
254  
255 GROUP  
256 SYNONYMS ARE:  
257 CONTAINED IN:  
258 CONSISTS OF:  
259  
260  
261  
262  
263 GROUP  
264 SYNONYMS ARE:  
265 CONTAINED IN:  
266 CONSISTS OF:  
267  
268  
269  
270  
271  
272 GROUP  
273 DESCRIPTION:  
274  
275 CONTAINED IN:  
276  
277  
278 CONSISTS OF:  
279  
280  
281  
282

sub-obj-inc-audit-trail;  
  
date-time,  
consol-nr;  
  
inc-audit-information;  
incaudinfo;  
sub-obj-audit-trail;  
  
incident-type,  
date-time,  
consol-nr;  
  
obj-audit-information;  
objaudinfo;  
sub-inc-audit-trail;  
  
object-id,  
date-time,  
consol-nr;  
  
obj-inc-audit-information;  
objincaudinfo;  
sub-audit-trail;  
  
object-id,  
incident-type,  
date-time,  
consol-nr;  
  
obj-sec-level;

This is the security level for an object;  
object-information,  
create-object-request,  
change-obj-sec-level-request;  
  
classification-level,  
category-set;  
reference-monitor-database;

SUBSETTING-CRITERION FOR:  
USED BY:

## Security-control-example

## FORMATTED PROBLEM STATEMENT

```

283      check-sub-obj-sec-levels
284          TO DERIVE
285      USED BY:
286      create-object-information
287          TO DERIVE
288      USED BY:
289      delete-object-information
290          TO DERIVE
291
292  GROUP
293      SYNONYMS ARE:
294      CONTAINED IN:
295      CONSISTS OF:
296
297
298
299
300  GROUP
301      DESCRIPTION:
302          This is the current security level for a subject.;
303      CONTAINED IN:
304          subject-information,
305          change-sub-curr-sec-level-req,
306          create-subject-command;
307
308
309      CONSISTS OF:
310          classification-level,
311          category-set;
312          reference-monitor-data-base;
313
314  SUBSETTING-CRITERION FOR:
315      USED BY:
316      check-sub-obj-sec-levels
317          TO DERIVE
318
319  GROUP
320      SYNONYMS ARE:
321      CONTAINED IN:
322      CONSISTS OF:
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999

```

error-code;

object-information;

error-code;

sub-audit-information;

subauditinfo;

obj-inc-audit-trail;

subject-id,

date-time,

consol-nr;

sub-curr-sec-level;

subject-information,

change-sub-curr-sec-level-req,

create-subject-command;

classification-level,

category-set;

reference-monitor-data-base;

error-code;

sub-inc-audit-information;

subincauditinfo;

obj-audit-trail;

subject-id,

incident-type,

date-time,

consol-nr;

sub-max-sec-level;

## FORMATTED PROBLEM STATEMENT

324 DESCRIPTION;           This is the maximum security level for a subject.;

325

326 CONTAINED IN:       subject-information,

327                       create-subject-command,

328                       change-sub-max-sec-level-command;

329

330

331

332                       classification-level,

333                       category-set;

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

GROUP           sub-obj-audit-information;

SYNONYMS ARE:   subobjauditinfo;

CONTAINED IN:   inc-audit-trail;

CONSISTS OF:    subject-id,

                 object-id,

                 date-time,

                 consol-nr;

GROUP           sub-obj-inc-audit-information;

SYNONYMS ARE:   subobjincauditinfo;

CONTAINED IN:   dump-audit-trail;

CONSISTS OF:    subject-id,

                 object-id,

                 incident-type,

                 date-time,

                 consol-nr;

EOF EOF EOF EOF EOF

KWIC INDEX

PARAMETERS FOR: KWIC

DIP=20 FILE

SEQ N A M F (PERMUTED)

1 attribute	usage
2 audit-information	inc
3 audit-information	obj
4 audit-information	sub
5 audit-information	obj-inc
6 audit-information	sub-inc
7 audit-information	sub-obj
8 audit-information	sub-obj-inc
9 audit-information	
10 category-set	
11 classification-level	error
12 code	validation
13 code	
14 consol-nr	sub
15 curr-sec-level	
16 date-time	
17 decision-type	
18 error-code	
19 id	object
20 id	subject
21 id	security
22 id	receiving-subject
23 id	requesting-subject
24 inc-audit-information	obj
25 inc-audit-information	sub
26 inc-audit-information	sub-obj
27 inc-audit-information	
28 incident-type	audit
29 information	inc-audit
30 information	obj-audit
31 information	sub-audit
32 information	obj-inc-audit
33 information	sub-inc-audit
34 information	sub-obj-audit
35 information	

## Security-control-example

## KWIC INDEX

## SEQ N A M E (PERMUTED)

36	information	sub-obj-inc-audit
37	level	obj-sec
38	level	sub-max-sec
39	level	sub-curr-sec
40	level	classification
41	location	object
42	max-sec-level	sub
43	nr	consol
44	obj-audit-information	
45	obj-audit-information	sub
46	obj-inc-audit-information	
47	obj-inc-audit-information	sub
48	obj-sec-level	
49	object-id	
50	object-location	
51	receiving-subject-id	obj
52	requesting-subject-id	sub-max
53	sec-level	sub-curr
54	sec-level	
55	sec-level	
56	security-id	category
57	set	
58	sub-audit-information	
59	sub-curr-sec-level	
60	sub-inc-audit-information	
61	sub-max-sec-level	
62	sub-obj-audit-information	
63	sub-obj-inc-audit-information	
64	subject-id	
65	subject-id	
66	subject-id	
67	time	receiving
68	type	requesting
69	type	date
70	usage-attribute	decision
71	validation-code	incident



Security-control-example

CONSISTS MATRIX REPORT

ROW NAMES

COLUMN NAMES

31 get-execute-request	INPUT
32 get-read-write-request	INPUT
33 release-usage-attr-request	INPUT
34 give-usage-attr-request	INPUT
35 rescind-usage-attr-request	INPUT
36 create-object-request	INPUT
37 delete-object-request	INPUT
38 change-obj-sec-level-request	INPUT
39 sub-obj-audit-request	INPUT
40 obj-audit-request	INPUT
41 create-subject-command	INPUT
42 delete-subject-command	INPUT
43 change-sub-max-sec-level-command	INPUT
44 link-reference-monitor-command	INPUT
45 subject-information	ENTRY
46 change-sub-curr-sec-level-request	INPUT
47 sub-audit-request	INPUT
48 create-subject-response	OUTPUT
49 delete-subject-response	OUTPUT
50 change-sub-max-sec-level-response	OUTPUT
51 link-reference-monitor-response	OUTPUT
52 sub-obj-inc-audit-trail	OUTPUT
53 sub-obj-audit-trail	OUTPUT
54 sub-inc-audit-trail	OUTPUT
55 sub-audit-trail	OUTPUT
56 obj-inc-audit-trail	OUTPUT
57 obj-audit-trail	OUTPUT
58 inc-audit-trail	OUTPUT
59 dump-audit-trail	OUTPUT

THE ROWS ARE CONTAINED IN THE COLUMNS WITH \*S



CONSIST'S MATRIX REPORT

1	11111111112	22222222223	33333333334	44444444445	5555555555
1234567890	1234567890	1234567890	1234567890	1234567890	123456789
26	I	I	I	I	*I

## CONSTSTS MATRIX REPORT

\*\*\*THE NUMBER OF COLUMNS THAT CONTAIN THE ROWS\*\*

13	subject-id	TYPE	COUNT
8	object-id	ELEMENT	21
5	decision-type	ELEMENT	19
3	consol-nr	ELEMENT	11
4	date-time	ELEMENT	9
7	incident-type	ELEMENT	9
14	usage-attribute	ELEMENT	7
12	security-id	ELEMENT	4
15	validation-code	ELEMENT	4
1	category-set	ELEMENT	3
2	classification-level	ELEMENT	3
22	obj-sec-level	GROUP	3
22	sub-curr-sec-level	GROUP	3
24	sub-max-sec-level	GROUP	3
10	receiving-subject-id	ELEMENT	2
11	requesting-subject-id	ELEMENT	2
9	object-location	ELEMENT	1
16	audit-information	GROUP	1
17	inc-audit-information	GROUP	1
18	obj-audit-information	GROUP	1
19	obj-inc-audit-information	GROUP	1
21	sub-audit-information	GROUP	1
23	sub-inc-audit-information	GROUP	1
25	sub-obj-audit-information	GROUP	1
26	sub-obj-inc-audit-information	GROUP	1
6	error-code	ELEMENT	0

\*\*\*THE NUMBER OF ROWS CONTAINED IN THE COLUMNS\*\*

12	sub-obj-inc-audit-information	TYPE	COUNT
8	obj-inc-audit-information	GROUP	5
10	sub-inc-audit-information	GROUP	4
11	sub-obj-audit-information	GROUP	4
34	give-usage-attr-request	INPUT	4

CONSISTS MATRIX REPORT

35	rescind-usage-attr-request	INPUT	4
41	create-subject-command	INPUT	4
4	incident-information	ENTITY	3
5	inc-audit-information	GROUP	3
6	obj-audit-information	GROUP	3
9	sub-audit-information	GROUP	3
25	sub-obj-inc-audit-request	INPUT	3
28	object-information	ENTITY	3
29	get-read-request	INPUT	3
30	get-write-request	INPUT	3
31	get-execute-request	INPUT	3
32	get-read-write-request	INPUT	3
33	release-usage-attr-request	INPUT	3
36	create-object-request	INPUT	3
38	change-obj-sec-level-request	INPUT	3
43	change-sub-max-sec-level-comd	INPUT	3
45	subject-information	INPUT	3
1	sub-max-sec-level	ENTITY	3
2	sub-curr-sec-level	GROUP	2
3	obj-sec-level	GROUP	2
7	audit-information	GROUP	2
24	sub-inc-audit-request	INPUT	2
26	obj-inc-audit-request	INPUT	2
37	delete-object-request	INPUT	2
39	sub-obj-audit-request	INPUT	2
42	delete-subject-command	INPUT	2
46	change-sub-curr-sec-level-req	INPUT	2
13	get-read-decision	OUTPUT	1
14	get-write-decision	OUTPUT	1
15	get-execute-decision	OUTPUT	1
16	get-read-write-decision	OUTPUT	1
17	release-usage-attr-decision	OUTPUT	1
18	give-usage-attr-decision	OUTPUT	1
19	rescind-usage-attr-decision	OUTPUT	1
20	create-object-decision	OUTPUT	1
21	delete-object-decision	OUTPUT	1
22	change-sub-curr-sec-level-dec	OUTPUT	1
23	change-obj-sec-level-decision	OUTPUT	1
27	inc-audit-request	INPUT	1
40	obj-audit-request	INPUT	1
44	link-reference-monitor-comd	INPUT	1

## Security-control-example

## CONSISTS MATRIX REPORT

47	sub-audit-request	INPUT	1
48	create-subject-response	OUTPUT	1
49	delete-subject-response	OUTPUT	1
50	change-sub-max-sec-level-resp	OUTPUT	1
51	link-reference-monitor-resp	OUTPUT	1
52	sub-obj-inc-audit-trail	OUTPUT	1
53	sub-obj-audit-trail	OUTPUT	1
54	sub-inc-audit-trail	OUTPUT	1
55	sub-audit-trail	OUTPUT	1
56	obj-inc-audit-trail	OUTPUT	1
57	obj-audit-trail	OUTPUT	1
58	inc-audit-trail	OUTPUT	1
59	dump-audit-trail	OUTPUT	1

## PROCESS INPUT/OUTPUT

PARAMETERS FOR: PRIO

NAME=delete-object INPUT OUTPUT DESCRIPTION PROCEDURE NONNEW-PAGE NOINDEX PRINT NOPUNCH

1\* delete-object

This process decides whether or not subject with  
subject-id may delete an object with object-id from the  
appropriate set in the reference monitor data base.

\*\*\* INPUTS \*\*\*

1 delete-object-request USED

\*\*\* OUTPUTS \*\*\*

1 delete-object-decision DERIVED

Security-control-example

CHANGE-TYPE REPORT

PARAMETERS FOR: CHANGE-TYPE

FILE TYPE=GROUP

1\* classification-level

OLD TYPE - ELEMENT

NEW TYPE - GROUP

2\* category-set

OLD TYPE - ELEMENT

NEW TYPE - GROUP

3\* subject-id

OLD TYPE - ELEMENT

NEW TYPE - GROUP

4\* object-id

OLD TYPE - ELEMENT

NEW TYPE - GROUP

5\* date-time

OLD TYPE - ELEMENT

NEW TYPE - GROUP

URA VERSION 3.021

Security-control-example

JUN 16, 1976 00:49:28

PAGE

20

REFNAME REPORT

PARAMETERS FOR: RPN

INPUT

SEQ OLD NAME

- 1 security-control-input
- 2 security-control-data-base

NEW NAME

- security-control-inputs
- security-control-data-bases

## Security-control-example

DELETED COMMENT ENTRIES

## PARAMETERS FOR: DCOM

DESCRIPTION NOPROCEDURE NOVOLATILITY NOVOLATILITY-MEMBER NOVOLATILITY-SET NO DERIVATION  
NOTRUE-WHILE NOFALSE-WHILE PRINT FILE

1\* security-control-data-bases  
DESCRIPTION;

1  
2  
3

The information in this set consists of all  
data stored and maintained by the security control  
system. ;

2\* security-control-interface  
DESCRIPTION;

1  
2  
3  
4  
5  
6

There will be several different types of users  
generating requests on the system and retrieving  
data from it. The security controls of the system  
must be capable of allowing users of different  
authorizations to process concurrently while preventing  
the release of information to unauthorized users. ;

3\* security-control-output  
DESCRIPTION;

1  
2  
3  
4

The system will produce outputs of several  
different types: approvals to data access or modification  
requests, audit trails on security features, a  
record of outputs produced, etc. ;

URA VERSION 3.0R1

Security-control-example

JUN 16, 1976 00:49:28

PAGE

21

D E L E T I O N

PARAMETERS FOR: DEL

FILE

DELETED - security-control-interface  
DELETED - security-control-system  
DELETED - security-control-inputs  
DELETED - security-control-output

R E P L A C E D C O M M E N T E N T R I E S

PARAMETERS FOR: PCOM

PRINT

' DELETED COMMENT ENTRY \*\*  
1\* sub-max-sec-level

DESCRIPTION :

1

This is the maximum security level for a subject.;

' INSERTED COMMENT ENTRY \*\*  
1\* sub-max-sec-level

DESCRIPTION :

1

2

3

This is the maximum security level for a subject.  
This subject must never be allowed to access an object  
which exceeds this security level.;

Security-control-example

DELETED URL

PARAMETERS FOR: DPSL

SOURCE NOXREF

LINE S T M T

YD FIELD

```

1 >ENTITY:      objinfo;
2 >      CONSISTS:  object-location;
3 >OUTPUT:      dump-audit-trail;
4 >      HAPPENS:   number-of-dump-audit   TIMES-PER month;
5 >PD:          michel-j-bastarache;
6 >      MAILBOX:   isdos-project-ann-anchor;
7 >EOF

```

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

FILE VOINDEX PRINT WOPUNCH SMARG=5 VMARG=20 AMARG=10 BMARG=25 CMARG=70 DMARG=40 DESG  
ONE-PER-LINE DEFINE COMMENT NONNEW-PAGE NONNEW-LINE

1 GROUP  
2 DESCRIPTION:  
3 This is a level of classification which may  
4 range up from unclassified to top secret and may be  
5 owned by a subject or an object.;  
6 SEE-MEMO: clearance-memo;  
7 CONTAINED IN: sub-max-sec-level,  
8 sub-curr-sec-level,  
9 obj-sec-level;  
10

classification-level;

11 GROUP  
12 DESCRIPTION:  
13 This is a set of categories of information which  
14 may be owned by a subject or an object.;  
15 SEE-MEMO: category-set-memo;  
16 CONTAINED IN: sub-max-sec-level,  
17 sub-curr-sec-level,  
18 obj-sec-level;  
19

category-set;

20 GROUP  
21 DESCRIPTION:  
22 This is a unique identifier for a subject.;  
23 CONTAINED IN: subject-information,  
24 get-read-request,  
25 get-write-request,  
26 get-execute-request,  
27 get-read-write-request,  
28 release-usage-attr-request,  
29 create-object-request,  
30 delete-object-request,  
31 change-sub-curr-sec-level-req,  
32 change-obj-sec-level-request,  
33 create-subject-command,  
34 delete-subject-command,  
35 change-sub-max-sec-level-command,  
36 sub-obj-audit-request,

subject-id;

## FORMATTED PROBLEM STATEMENT

37 sub-inc-audit-request,  
 38 sub-obj-inc-audit-request,  
 39 sub-audit-request,  
 40 sub-audit-information,  
 41 sub-inc-audit-information,  
 42 sub-obj-audit-information,  
 43 sub-obj-inc-audit-information;  
 44 subject-information;

## IDENTIFIERS:

USED BY:

45 check-need-to-know-usage  
 46 TO DERIVE error-code;

USED BY:

48 check-access-usage  
 49 TO DERIVE error-code;

USED BY:

51 delete-access-relation  
 52 TO DERIVE error-code;

USED BY:

53 create-access-relation  
 54 TO UPDATE usage-attribute;

## GROUP

DESCRIPTION:

object-id:

This is a unique identifier for an object.:

CONTAINED IN:

60 object-information,  
 61 get-read-request,  
 62 get-write-request,  
 63 get-execute-request,  
 64 get-read-write-request,  
 65 release-usage-attrib-request,  
 66 give-usage-attrib-request,  
 67 reset-usage-attrib-request,  
 68 create-object-request,  
 69 delete-object-request,  
 70 change-obj-sec-level-request,  
 71 sub-obj-audit-request,  
 72 obj-audit-information,  
 73 sub-obj-inc-audit-request,  
 74 obj-inc-audit-information,  
 75 obj-inc-audit-request,  
 76 obj-audit-request,

77

## FORMATTED PROBLEM STATEMENT

78 sub-bbj-audit-information,  
 79 sub-bbj-inc-audit-information;  
 80 IDENTIFIERS: object-information;  
 81 USED BY:

82 check-need-to-know-usage  
 83 TO DERIVE error-code;  
 84 USED BY:

85 check-access-usage  
 86 TO DERIVE error-code;  
 87 USED BY:

88 delete-access-relation  
 89 TO DERIVE error-code;  
 90 USED BY:

91 create-object-information  
 92 TO DERIVE object-information;  
 93 USED BY:

94 delete-object-information  
 95 TO DERIVE error-code;  
 96 USED BY:

97 create-access-relation  
 98 TO UPDATE usage-attribute;  
 99

100 GROUP date-time;

101 DESCRIPTION;

102 This is the date and time an audit incident  
 103 occurred.;

104 CONTAINED IN: incident-information,  
 105 inc-audit-information,  
 106 bbj-audit-information,  
 107 audit-information,  
 108 bbj-inc-audit-information,  
 109 sub-audit-information,  
 110 sub-inc-audit-information,  
 111 sub-bbj-audit-information,  
 112 sub-bbj-inc-audit-information;  
 113

114 SET

security-control-data-bases;

115 SYNONYMS ARE: scdb;

116 SEE-MEMO: system-philosophy-memo;

117 KEYWORDS: level-1;

118 ATTRIBUTES ARE:

## FORMATTED PROBLEM STATEMENT

```

119 specification-derivation
120 implicit;
121 SUBSETS ARE: reference-monitor-data-base,
122 auditing-system-data-base;
123 SECURITY IS: unclassified;
124
125 /* NAME NOT FOUND IN DB-          security-control-inputs
126 */
127
128 /* NAME NOT FOUND IN D3-          SCS
129 */
130
131 GROUP
132 DESCRIPTION:
133 This is the maximum security level for a subject.
134 This subject must never be allowed to access an object
135 which exceeds this security level.;
136 CONTAINED IN: subject-information,
137 create-subject-command,
138 change-sub-max-sec-level-com1;
139
140 CONSISTS OF:
141 classification-level,
142 category-set;
143
144 DESIGNATE AS A SYNONYM FOR object-information;
145
146 OUTPUT
147 SYNONYMS ARE: dumpaudit;
148 PART OF: audit-trail;
149 CONSISTS OF:
150 number-of-incidents
151 sub-obj-inc-audit-information;
152 DERIVED BY: dump-audit;
153
154 PROBLEM-DEFINER
155 RESPONSIBLE FOR:
156 auditing-system,
157 administrative-security-system,
158 reference-monitor,
159 system-security-administrator;
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

URA VERSION 3.031

PAGE 217

JUN 16, 1976 00:49:28

Security-control-example

FORMATTED PROBLEM STATEMENT

160

161 EOF EOF EOF EOF EOF

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='KEY=level-2 AND PROCESS' ORDER=BY TYPE

- |   |                                |         |
|---|--------------------------------|---------|
| 1 | administrative-security-system | PROCESS |
| 2 | auditing-system                | PROCESS |
| 3 | reference-monitor              | PROCESS |

## Name Generation

## PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='( NOT PROCESS ) \* KEY=level-2' ORDER=BYTYPE

1	administrative-security-comd	INPUT
2	auditing-request	INPUT
3	reference-monitor-request	INPUT
4	reference-monitor-subject	INTERFACE
5	system-security-administrator	INTERFACE
6	administrative-security-resp	OUTPUT
7	audit-trail	OUTPUT
8	reference-monitor-decision	OUTPUT
9	auditing-system-data-base	SET
10	reference-monitor-data-base	SET

University of Michigan - MFS

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ATTR=occurrences,unscheduled AND SO=security-control-input',  
ORDER=BYTYPE

- |   |                              |       |
|---|------------------------------|-------|
| 1 | administrative-security-comd | INPUT |
| 2 | reference-monitor-request    | INPUT |

TRA VERSION 3.001

PAGE 221

JUL 19, 1976 15:07:44  
University of Michigan - MFS

Name Generation

PARAMETERS POP: NG

PRINT PUNCH EMPTY SELECTION=' (INPUT OR OUTPUT) \* ATTR=specder,implicit' ORDER=BYTYPE

- |   |                         |        |
|---|-------------------------|--------|
| 1 | security-control-input  | INPUT  |
| 2 | security-control-output | OUTPUT |

## PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='SO=security-control-input OR SO=security-control-output',  
ORDER=BYTYPE

## Name Generation

1	administrative-security-comd	INPUT
2	auditing-request	INPUT
3	change-obj-sec-level-request	INPUT
4	change-sub-curr-sec-level-req	INPUT
5	change-sub-max-sec-level-comd	INPUT
6	create-object-request	INPUT
7	create-subject-command	INPUT
8	delete-object-request	INPUT
9	delete-subject-command	INPUT
10	dump-audit-request	INPUT
11	get-execute-request	INPUT
12	get-read-request	INPUT
13	get-read-write-request	INPUT
14	get-write-request	INPUT
15	give-usage-attr-request	INPUT
16	inc-audit-request	INPUT
17	link-reference-monitor-comd	INPUT
18	obj-audit-request	INPUT
19	obj-inc-audit-request	INPUT
20	reference-monitor-request	INPUT
21	release-usage-attr-request	INPUT
22	rescind-usage-attr-request	INPUT
23	sub-audit-request	INPUT
24	sub-inc-audit-request	INPUT
25	sub-obj-audit-request	INPUT
26	sub-obj-inc-audit-request	INPUT
27	administrative-security-resp	OUTPUT
28	audit-trail	OUTPUT
29	change-obj-sec-level-decision	OUTPUT
30	change-sub-curr-sec-level-dec	OUTPUT
31	change-sub-max-sec-level-resp	OUTPUT
32	create-object-decision	OUTPUT
33	create-subject-response	OUTPUT
34	delete-object-decision	OUTPUT
35	delete-subject-response	OUTPUT
36	dump-audit-trail	OUTPUT

## Name Generation

37	get-execute-decision	OUTPUT
38	get-read-decision	OUTPUT
39	get-read-write-decision	OUTPUT
40	get-write-decision	OUTPUT
41	give-usage-attr-decision	OUTPUT
42	inc-audit-trail	OUTPUT
43	link-reference-monitor-resp	OUTPUT
44	obj-audit-trail	OUTPUT
45	obj-inc-audit-trail	OUTPUT
46	reference-monitor-decision	OUTPUT
47	release-usage-attr-decision	OUTPUT
48	rescind-usage-attr-decision	OUTPUT
49	sub-audit-trail	OUTPUT
50	sub-inc-audit-trail	OUTPUT
51	sub-obj-audit-trail	OUTPUT
52	sub-obj-inc-audit-trail	OUTPUT

## INDEX

URA Report	Page(s) found in Output
-----	-----
AS-IS SOURCE LISTING .....	1, 3, 6, 14, 23, 41, 75, 96, 109, 123
ATTRIBUTE REPORT .....	143
CHANGE TYPE .....	227
CONSISTS COMPARISON MATRIX .....	63
CONSISTS MATRIX .....	199
CONTENTS REPORT .....	57
CROSS REFERENCE .....	7
DATA BASE SUMMARY .....	27, 55, 87, 100, 113, 126
DATA PROCESS REPORT .....	89
DELETED COMMENT ENTRIES .....	209
DELETED URL .....	212
DELETION .....	210
DICTIONARY .....	131
EXTENDED PICTURE .....	94
FORMATTED PROBLEM STATEMENT .....	9, 18, 33, 73, 102, 105, 118, 122, 128, 147, 163, 172, 181, 194, 188, 213
FREQUENCY REPORT .....	108
IDENTIFIER INFORMATION REPORT .....	70
INDEX .....	60
KWIC INDEX .....	197
NAME GENERATION .....	8, 17, 32, 35, 56, 62, 69, 72, 88, 101, 105, 117, 121, 127, 130, 133, 142, 146, 162, 171, 180, 183, 187, 218, 219, 220, 221, 222
NAME LIST .....	22, 136
PICTURE .....	10, 12, 36
PROCESS CHAIN .....	114
PROCESS INPUT/OUTPUT .....	206
PUNCHED COMMENT ENTRIES .....	134
RENAME .....	208
REPLACED COMMENT ENTRIES .....	211
STRUCTURE .....	28, 29, 30, 31, 144, 161, 170, 179